

FIG. 1

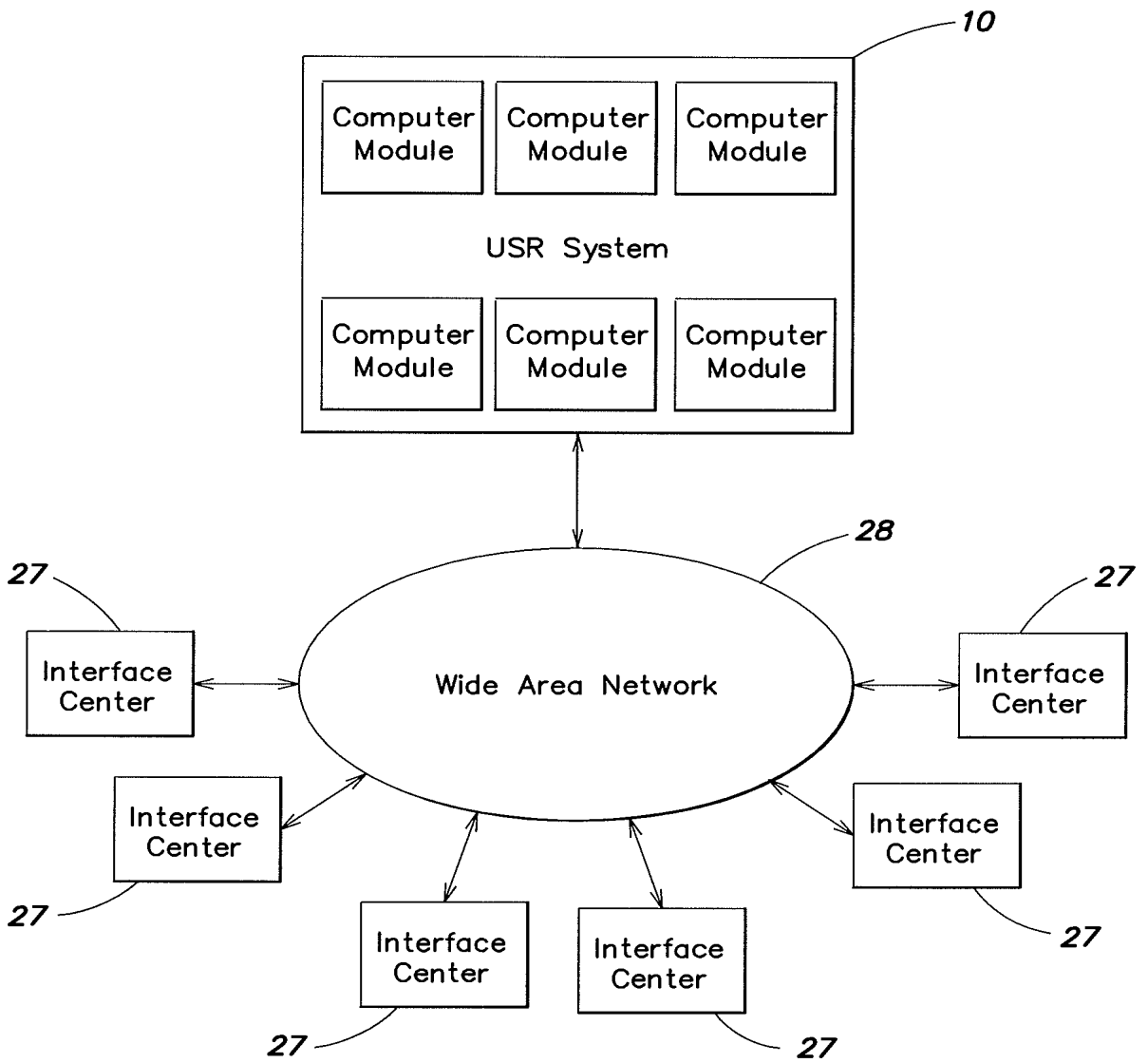


FIG. 2

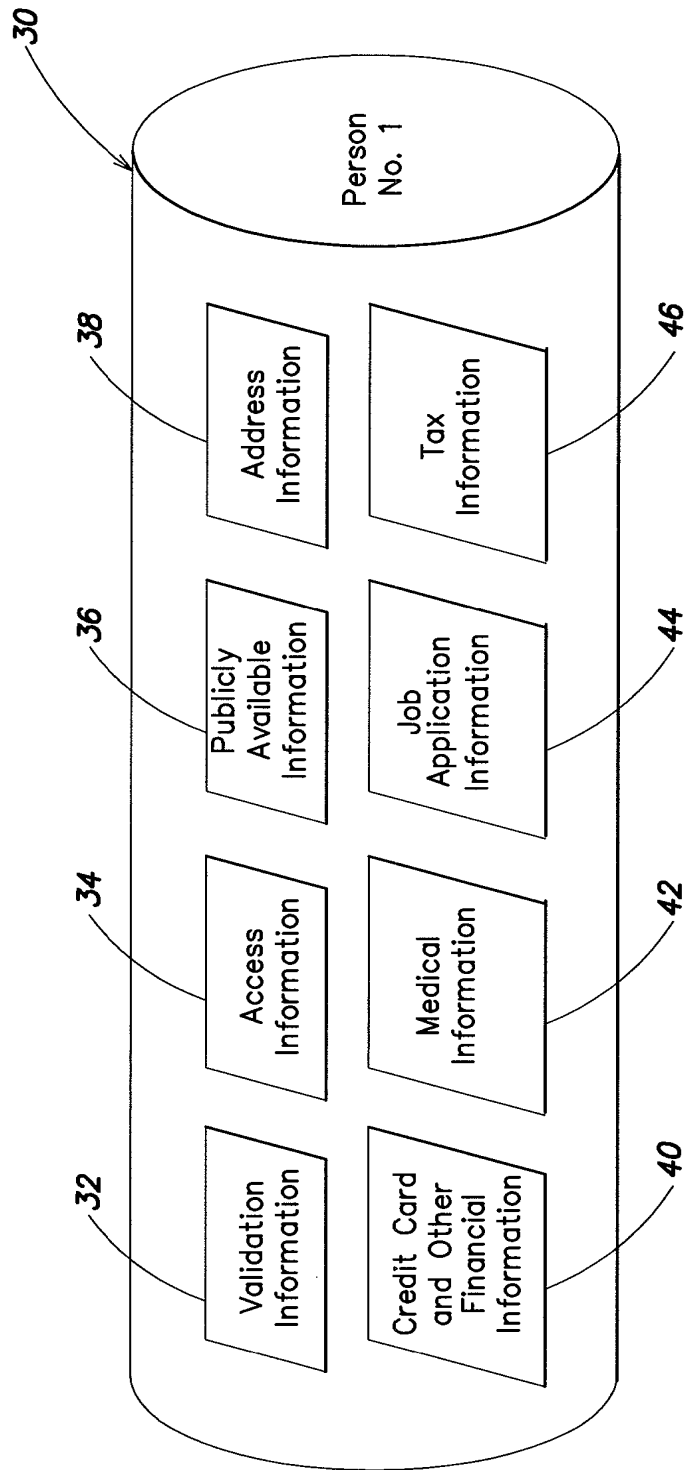


FIG. 3

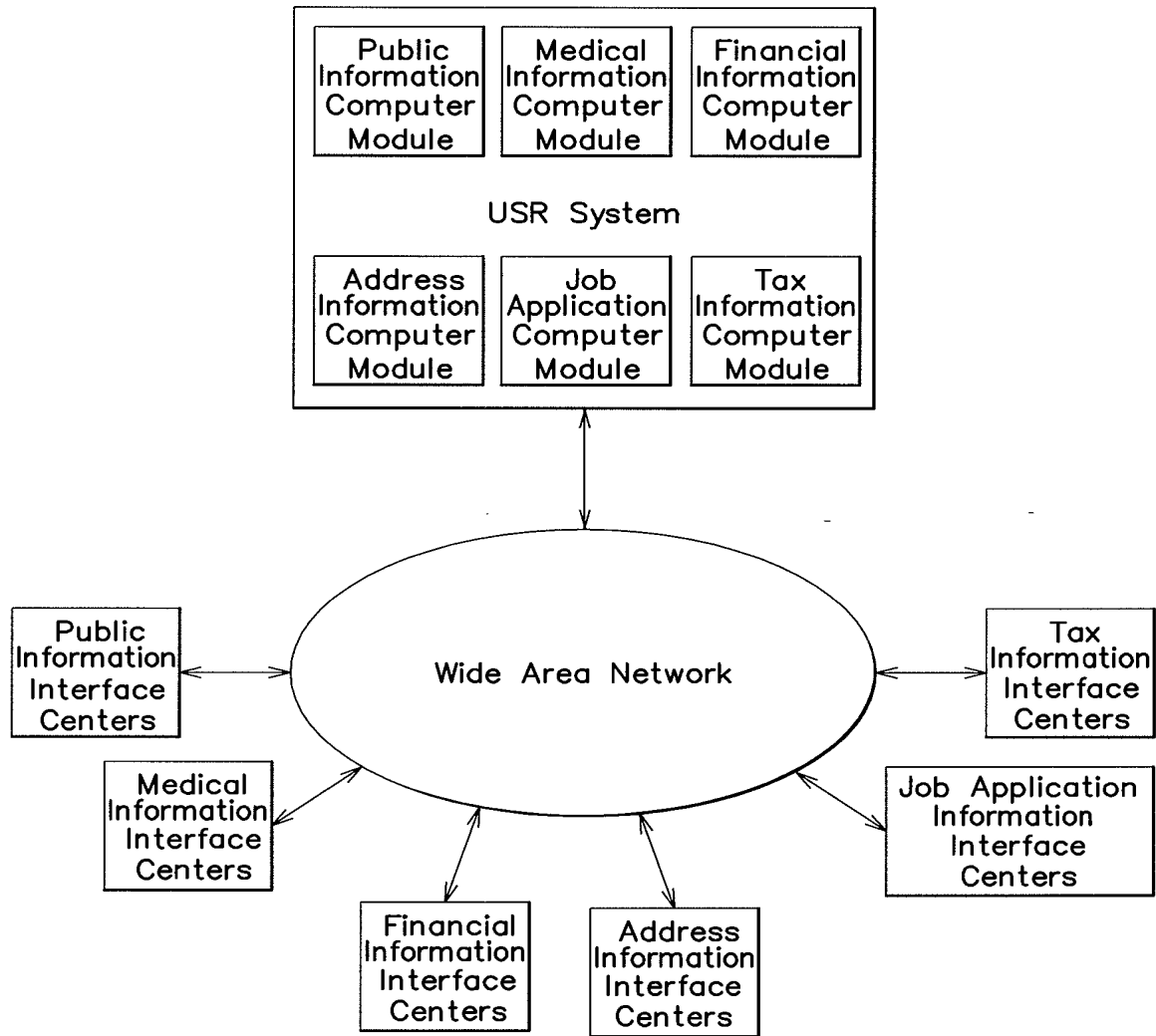


FIG. 4

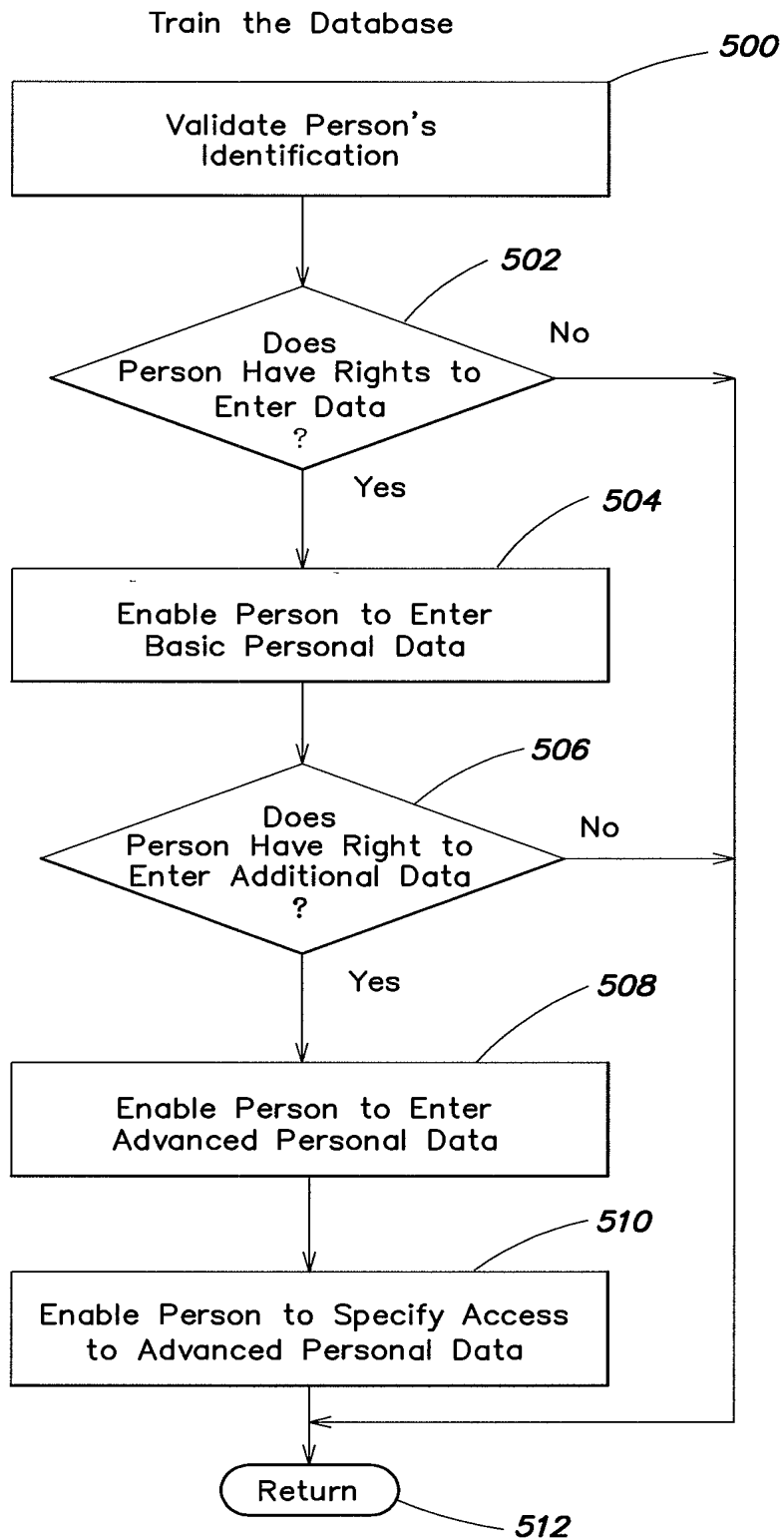


FIG. 5

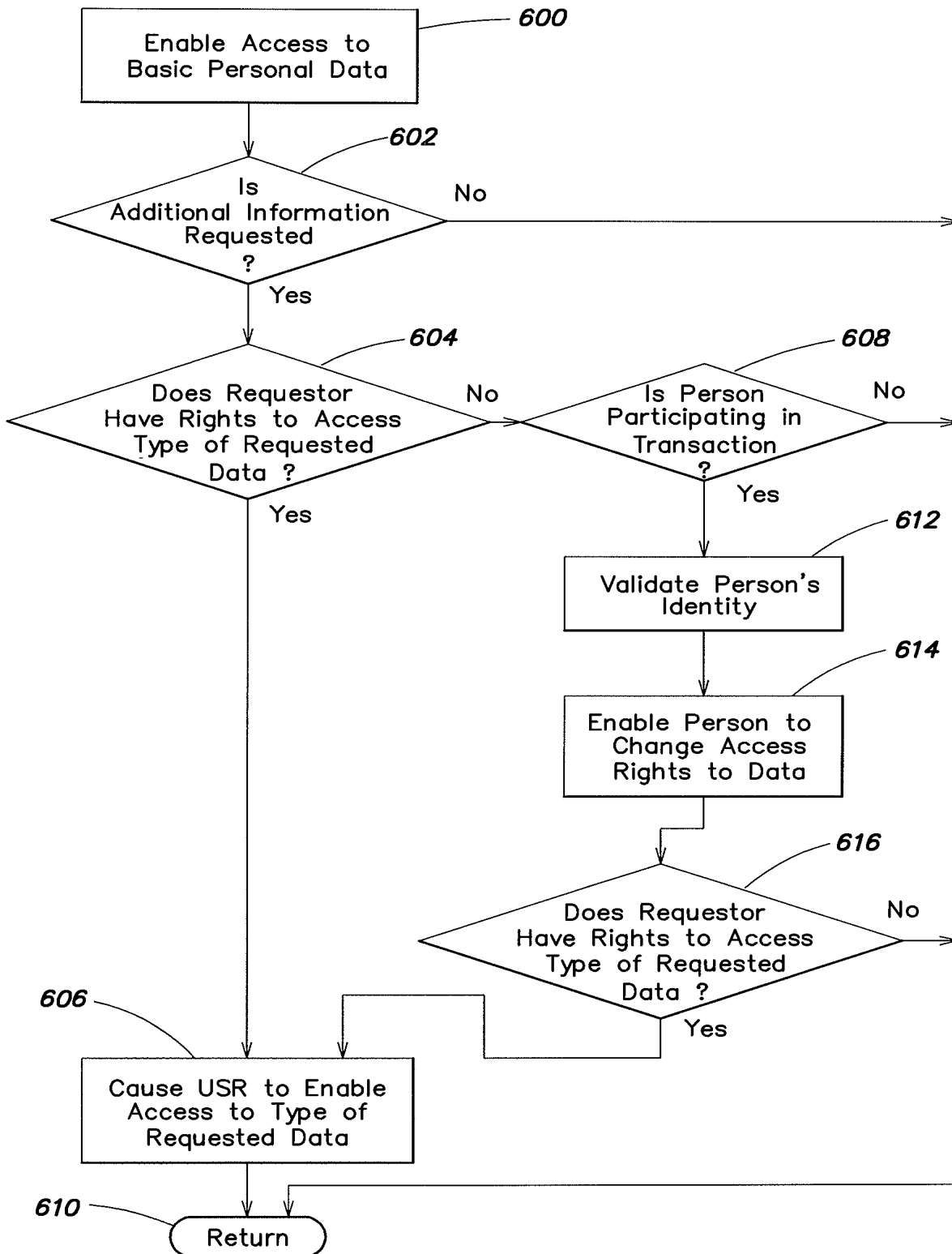


FIG. 6

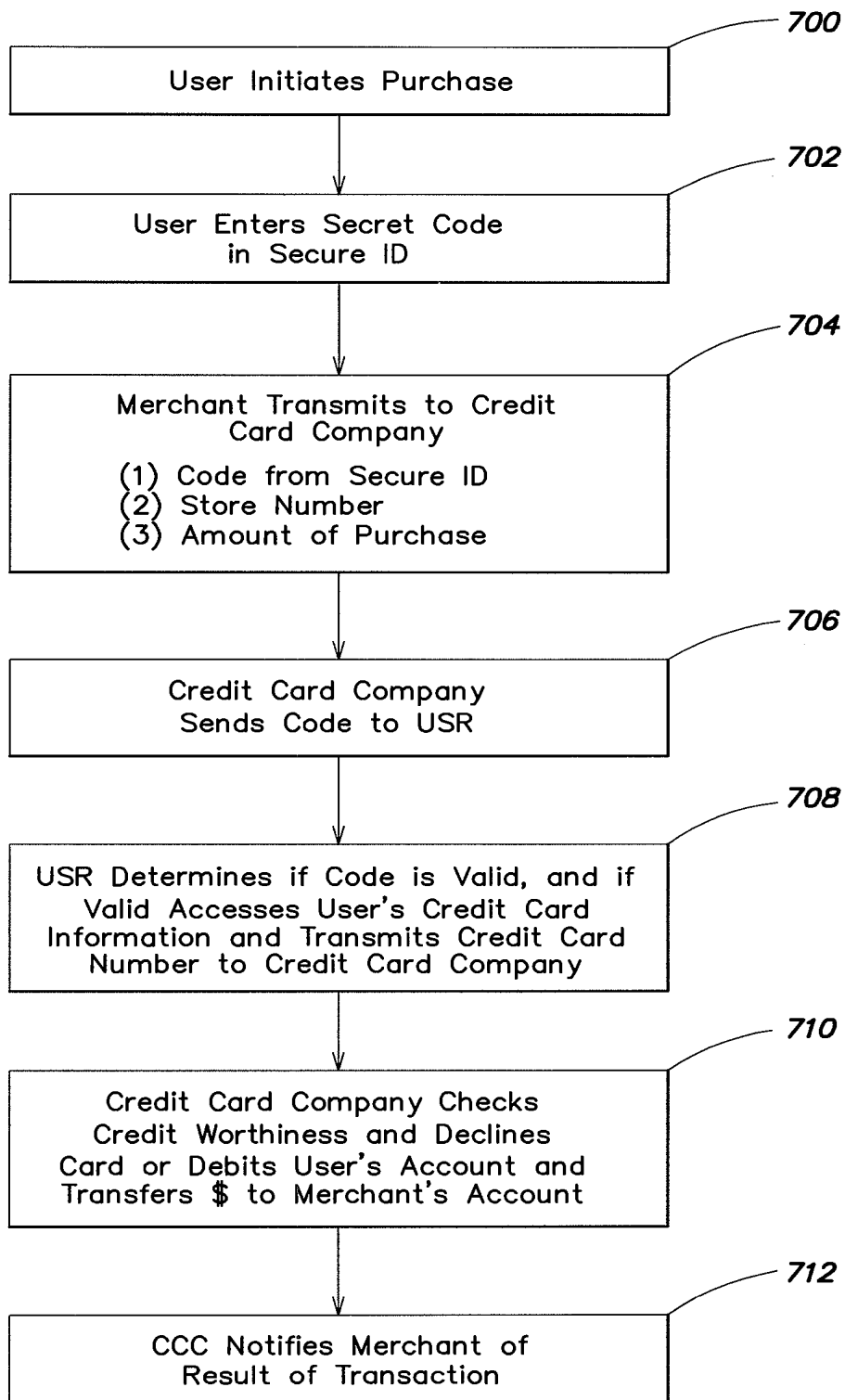


FIG. 7

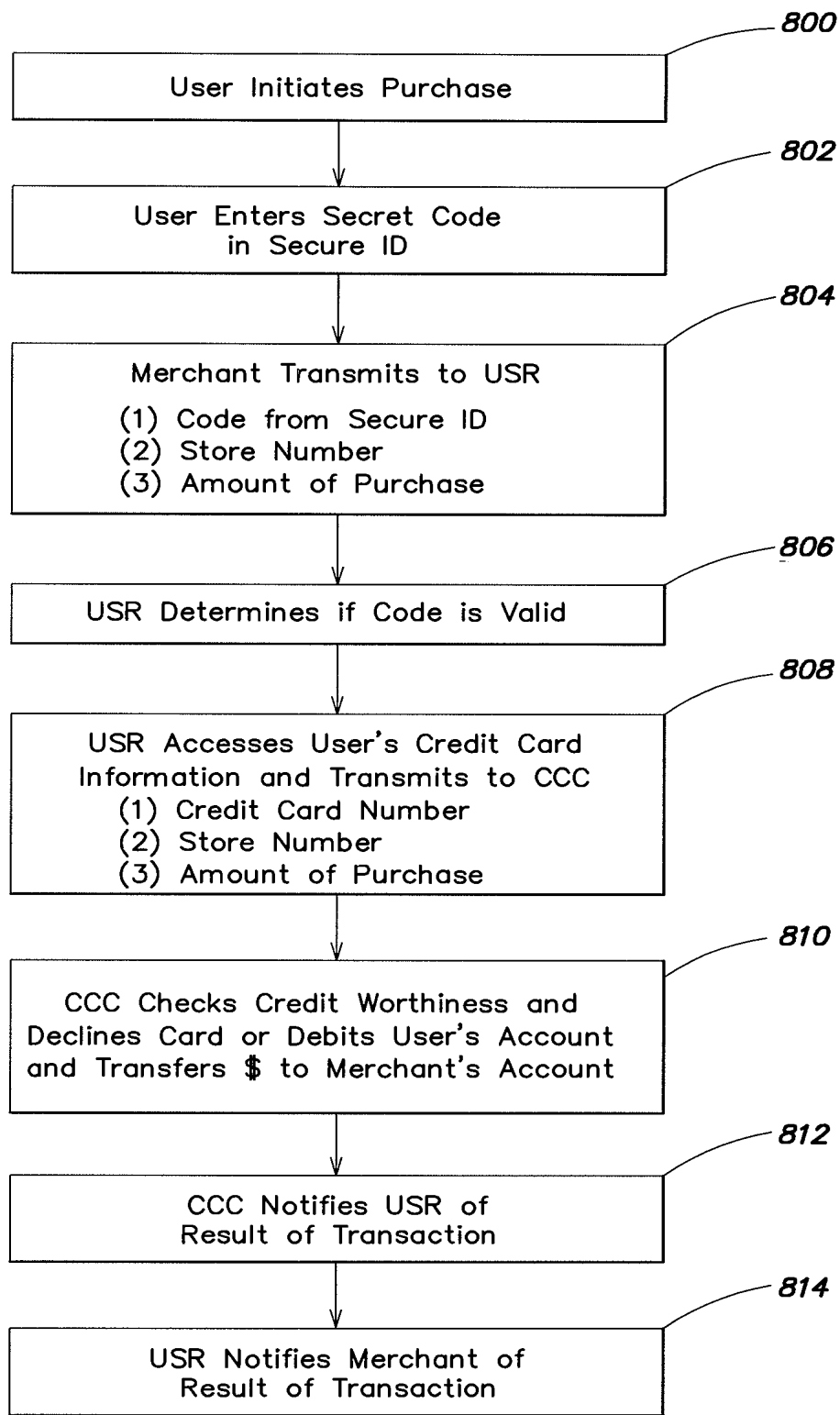


FIG. 8

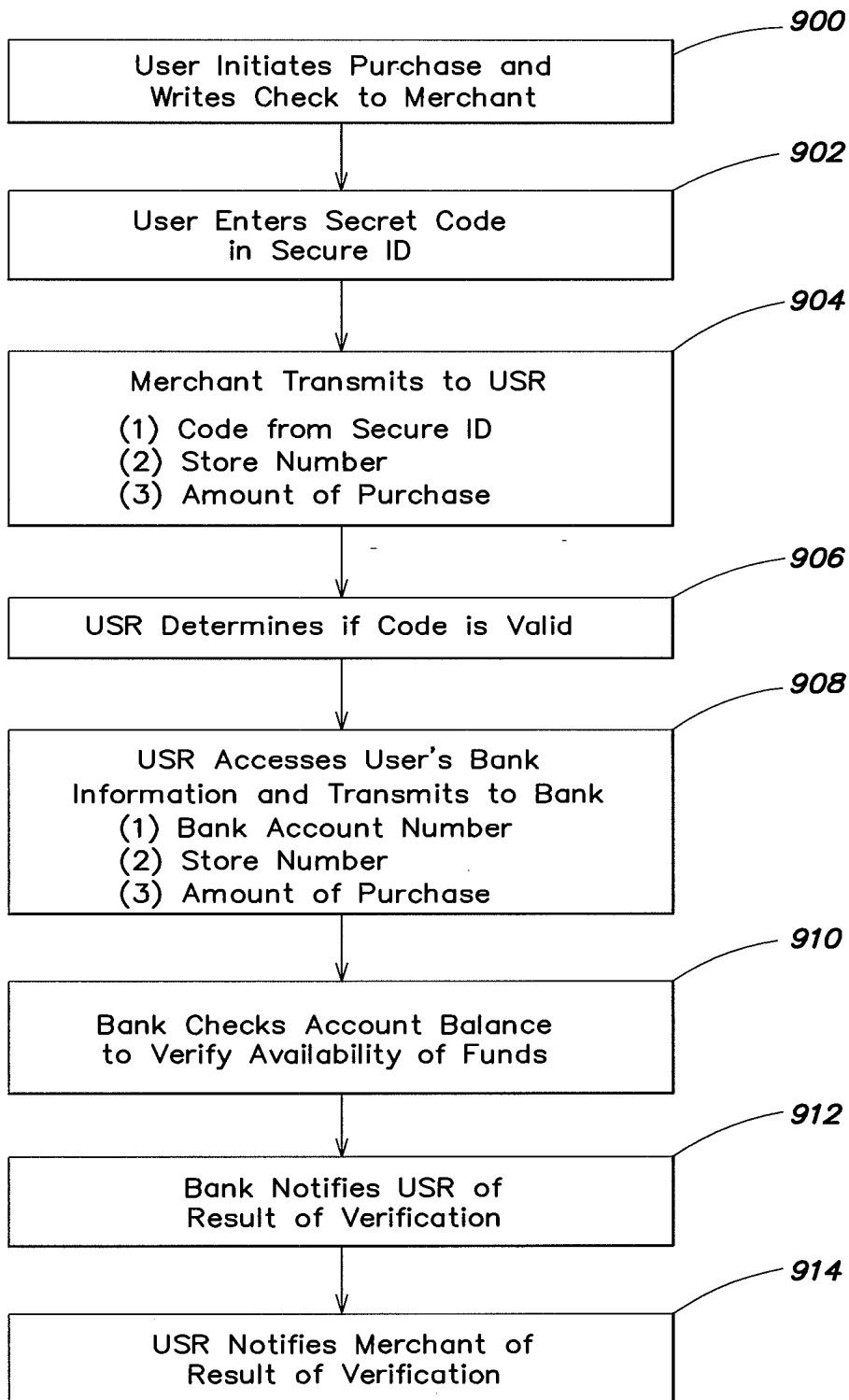


FIG. 9

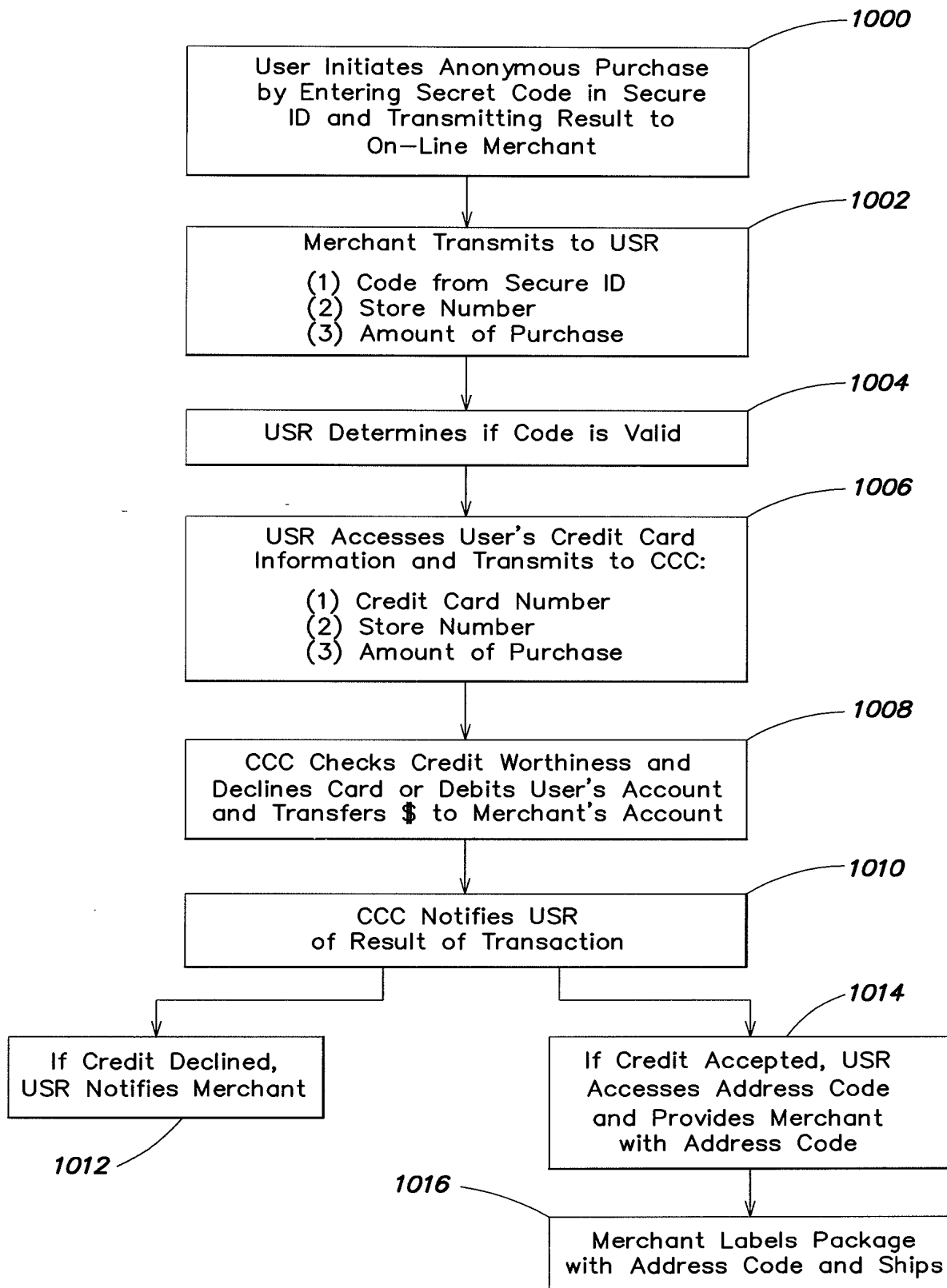


FIG. 10

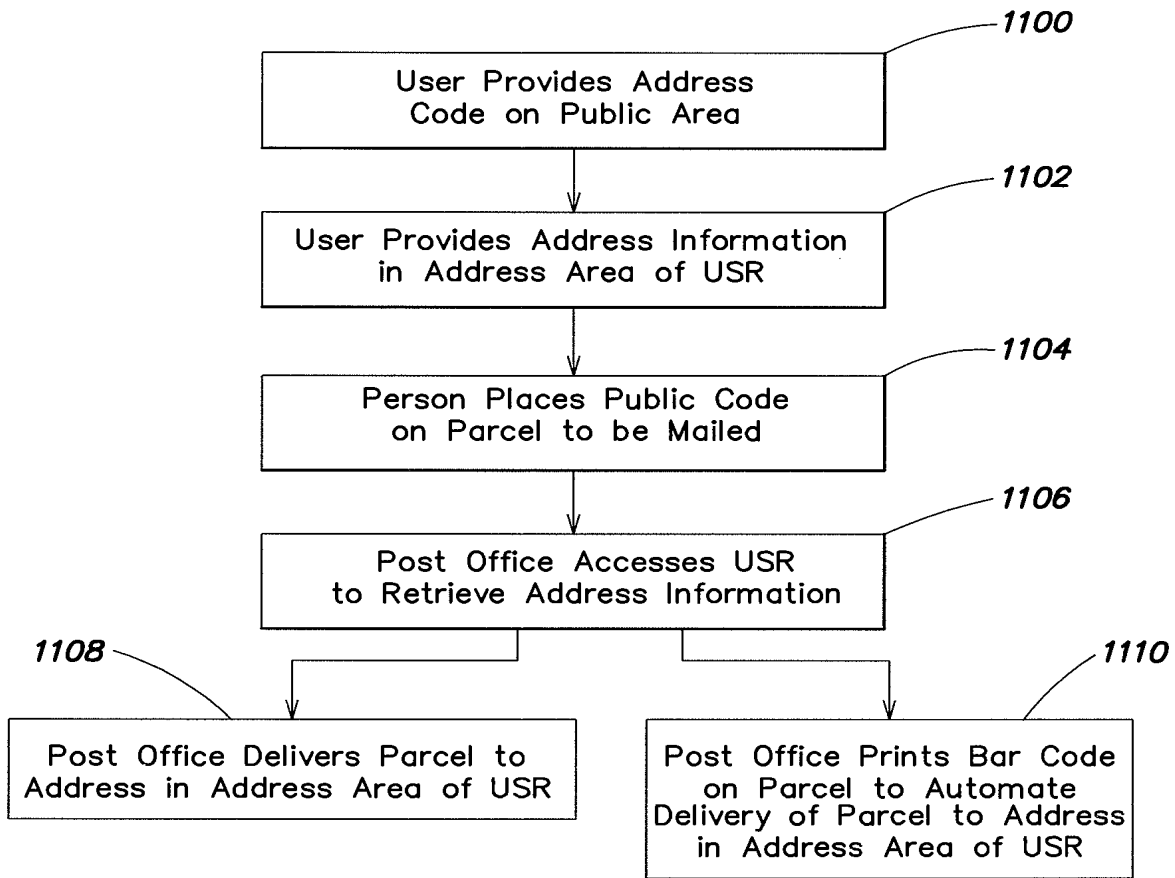


FIG. 11

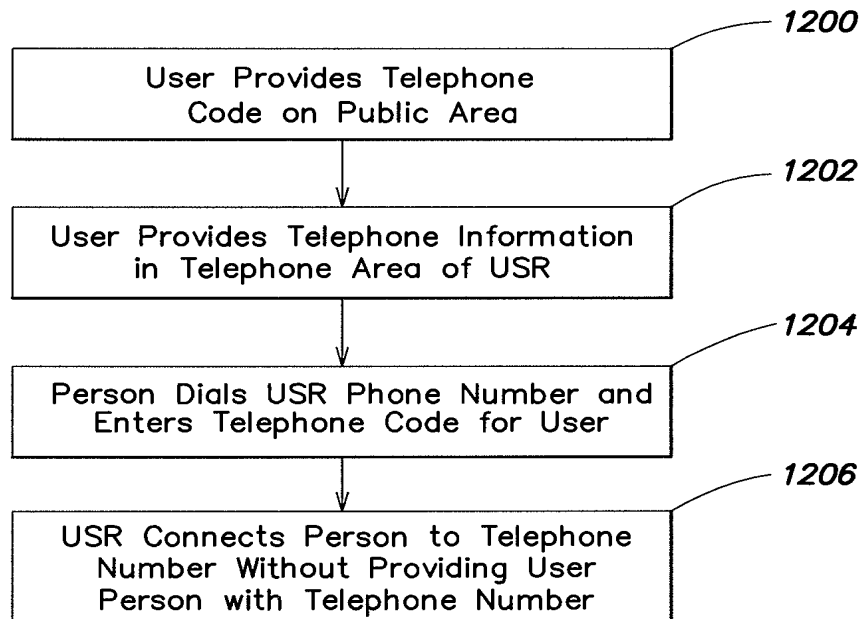


FIG. 12

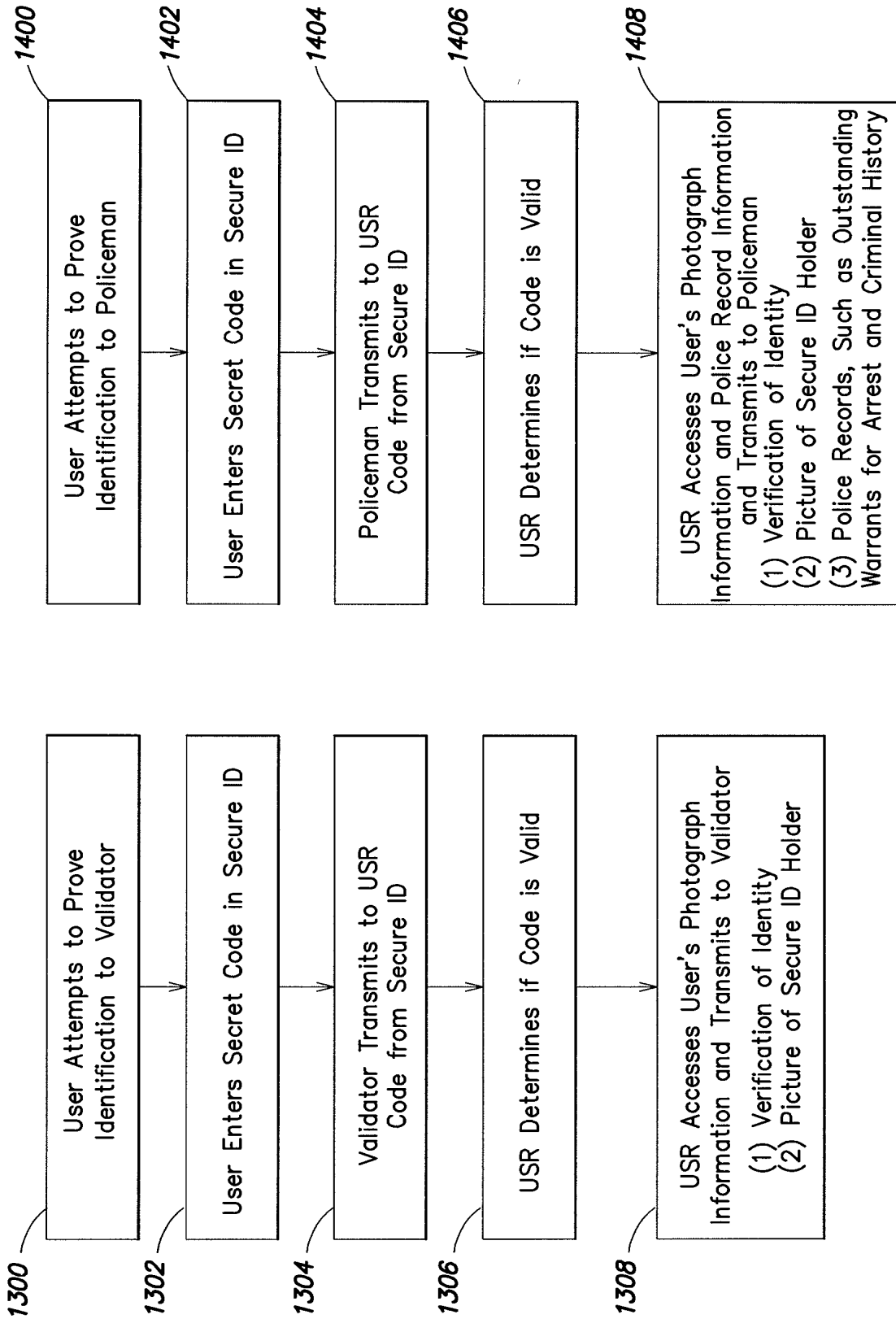


FIG. 14

FIG. 13

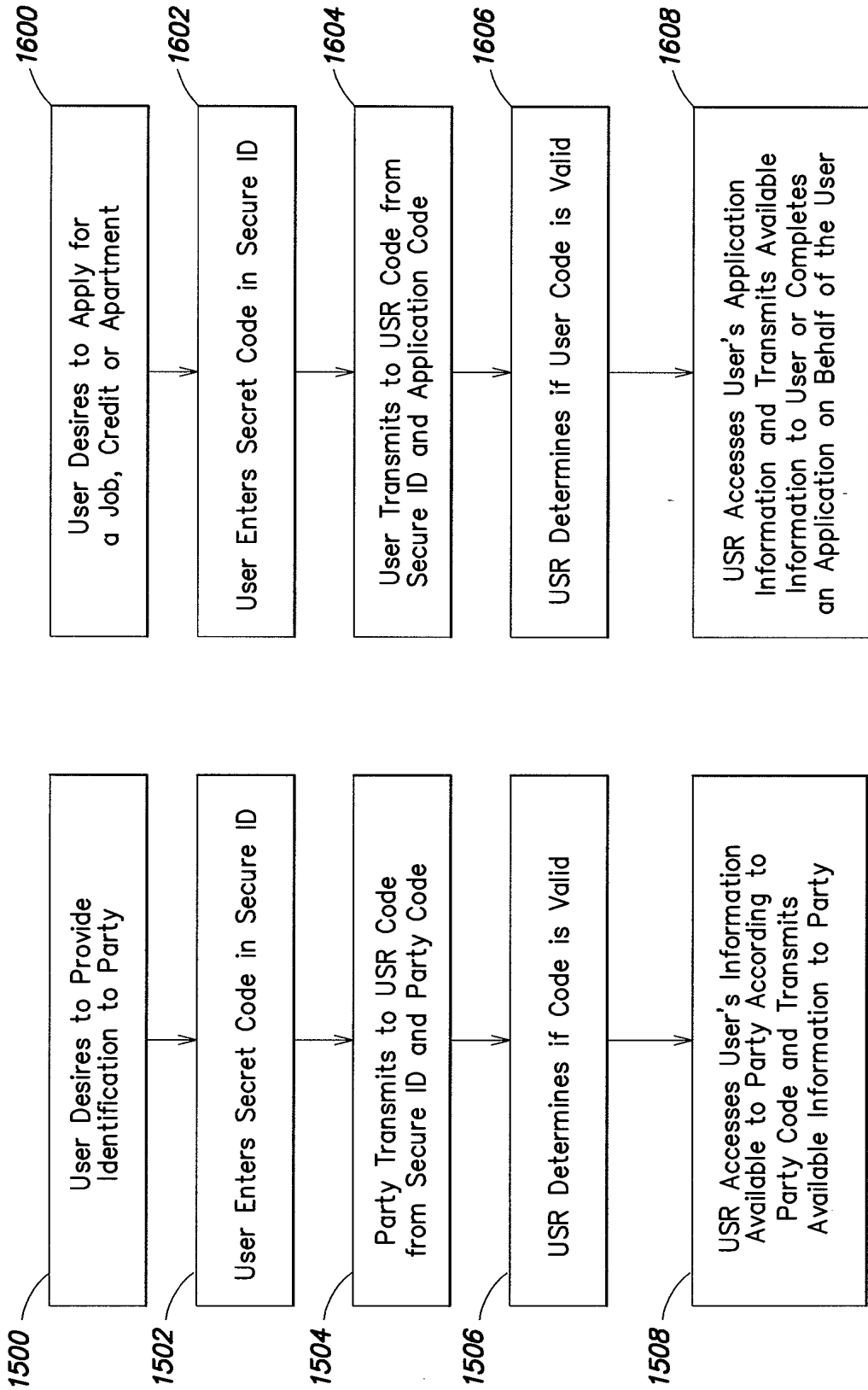


FIG. 15

FIG. 16

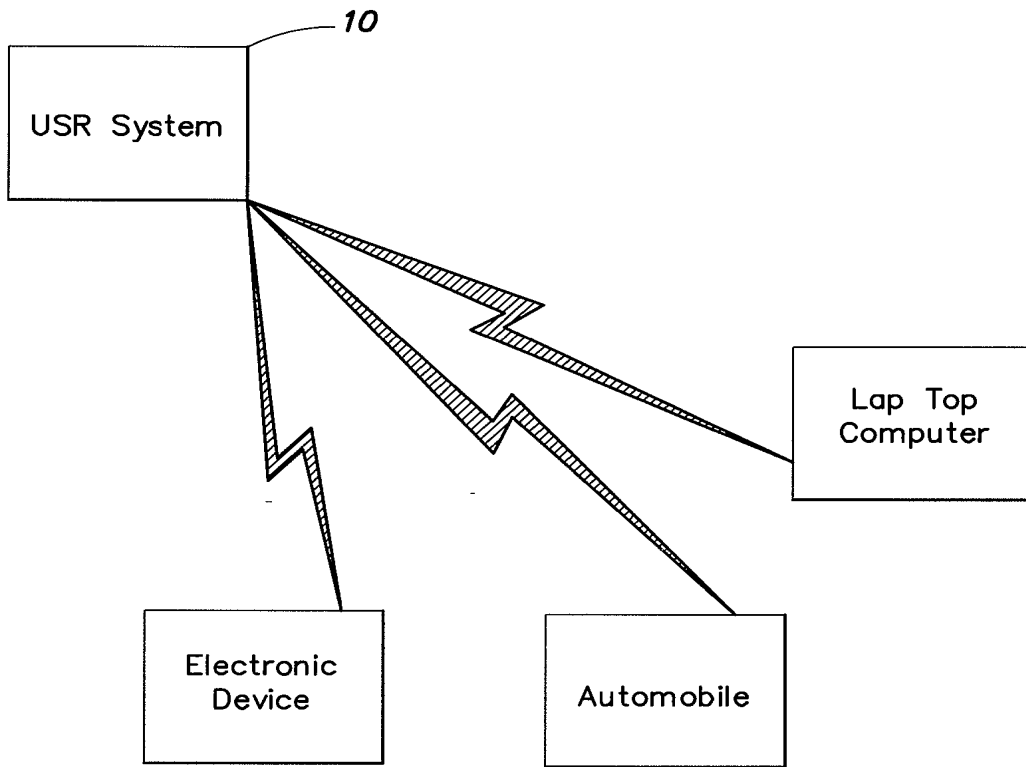


FIG. 17

UNIVERSAL SECURE REGISTRY

RELATED APPLICATIONS

5 This application claims the benefit under 35 U.S.C. § 120 of U.S. Application Serial
No. 09/810,703, filed on March 16, 2001 and issued on June 26, 200 as Patent No. 7,237,117,
which is herein incorporated by reference in its entirety.

BACKGROUND OF INVENTION

1. Field of Invention

10 This invention generally relates to a method and apparatus for securely storing and
disseminating information regarding individuals and, more particularly, to a computer system
for authenticating identity or verifying the identity of individuals and other entities seeking
access to certain privileges and for selectively granting privileges and providing other
services in response to such identifications/verifications.

15

2. Discussion of Related Art

Dissemination of information regarding various entities, including individuals, in
society is conventionally done in a non-centralized fashion, often requiring specialized
knowledge of a likely storage location to access the information. This specialized knowledge
20 may not be available when the information is needed, thus effectively preventing distribution
of the information when required. For example, a doctor in an emergency room may desire
access to a patient's medical history in determining a course of treatment. If the person is not
carrying a complete medical record, which is typically the situation, the medical records may
not be available to the doctor. Even if these medical records are available electronically, for
25 example via a computer accessible in the person's regular doctor's office, the records may
effectively be unavailable if the person is unconscious or otherwise incapacitated or if
restrictions on access to the doctor's records cannot otherwise be overcome. The retrieval of
required medical records can be further complicated by the fact that such records can be
located at a number of different sites/systems which are not linked. For example, the
30 patient's primary care physician may not have records from a specialist treating the patient,
and none of these physicians may have dental records. Similar problems arise in other

environments where relevant data may be scattered and/or otherwise difficult to access.

Identification of a person from other persons within a society and verification of a person as being who he says he is are extremely important for many reasons. For example, determination/verification of a person's identity will typically dictate extension of credit,
5 granting access to information, allowing entry to a restricted area, or the granting of numerous other privileges.

Most people carry multiple forms of identification. For example, a typical person may carry an identification card issued by a federal, state, or local governmental entity, an identification card issued by a university or place of employment, one or more credit cards
10 that serve to identify the person as a holder of a credit card account, one or more bank cards that serve to identify the person as holder of a bank account, medical information cards identifying the person as a member of, for example, a health maintenance organization or as a person holding an insurance policy from a specified insurance company, keys that identify the person as owner of an automobile, house, etc., and numerous other identification cards
15 that may be used for specialized purposes, such as identifying the person as a member of a health club, a library, or a professional organization.

To enable the person to function effectively in society, the person must typically have one or more of these identification devices with them if they wish to undertake an associated activity. For example, a person is not allowed to drive a car or purchase alcohol without a
20 governmentally issued driver's license. Likewise, although cash may be used to purchase goods and/or services, the person will typically not be able to purchase goods and/or services with a credit card if the person is not physically carrying the credit card. Similarly, most hospitals and other medical facilities will require proof of insurance before rendering medical attention. Carrying these multifarious identification devices can become onerous.
25 Additionally, if one or more of the identification devices is lost, stolen or forgotten, it can be inconvenient, making it difficult to obtain goods or services requiring the missing identification.

There are also times when the individual may wish to be identified or at least verified without providing personal information. For example, a person may wish to purchase goods
30 and/or services without publicly providing his/her credit card information for fear that the credit card information be may be stolen and used fraudulently. Likewise, the person may

wish to purchase goods or order goods to be delivered to an address without revealing the address to the vendor. Unfortunately, conventional identification devices require that at least some personal information be transmitted to complete a transaction.

5 There are other related problems. For example, when there is a need to locate a person or other entity where only limited biographical data is known, this can be difficult since relevant information is seldom available from a single database. Another potential problem is the forwarding of mail, packages, telephone calls/messages, e-mails and other items where a party is in a situation where they are changing location frequently and/or where the person does not want such information to be generally available for security or other reasons. A simple, yet secure, way of dealing with such issues does not currently exist.

10 Another potential problem is filling in forms, particularly for an individual who frequently has to complete the same or similar form. Such forms can for example be medical forms when visiting a doctor or entering a hospital, immigration forms on entering the country, employment forms, college entry forms, etc. It would be desirable if such forms could be completed once and be available for future use, and it would be even better if the information for each such form could be automatically drawn from an existing database to complete the form. There is also a frequent requirement to periodically update information in a form, for example financial information for a line of credit. It would be desirable if such updates could be automatically performed from data in a general database.

20 Still another potential problem is that a person may be forced to make requests on a database, for example financial requests, under duress. It would be desirable if the person could easily and undetectably signal such duress when making the request and the receiving system be able to act appropriately to assist and protect the individual.

25 Systems capable of effectively performing all of these functions do not currently exist.

SUMMARY OF INVENTION

There is thus a need for an identification system that will enable a person to be identified or verified (“identification” sometimes being used hereinafter to mean either identified or verified) and/or authenticated without necessitating the provision of any personal information. Likewise, there is a need for an identification system that will enable a person

to be identified universally without requiring the person to carry multiple forms of identification.

Accordingly, this invention relates, in one embodiment, to an information system that may be used as a universal identification system and/or used to selectively provide personal, financial or other information about a person to authorized users. Transactions to and from the database may take place using a public key/private key security system to enable users of the system and the system itself to encrypt transaction information during the transactions. Additionally, the private key/public key security system may be used to allow users to validate their identity and/or sign instructions being sent to a universal secure registry (USR) system of the type to which this invention relates. For example, in one embodiment, a smart card such as the SecurID™ card from RSI Security, Inc. may be provided with the user's private key and the USR system's public key to enable the card to encrypt messages being sent to the USR system and to decrypt messages from the USR system 10.

This USR system or database may be used to identify the person in many situations, and thus may take the place of multiple conventional forms of identification. Additionally, the USR system may enable the user's identity to be confirmed or verified without providing any identifying information about the person to the entity requiring identification. This can be advantageous where the person suspects that providing identifying information may subject the identifying information to usurpation.

Enabling anonymous identification facilitates multiple new forms of transactions. For example, enabling anonymous identification enables the identified person to be telephoned by or receive e-mails from other persons without providing the other person with a telephone number or e-mail address, and will permit this to be accomplished even where there are frequent changes in the person's location. Similarly, enabling anonymous identification will enable the person to receive mail, other delivered parcels and other items without providing the recipient's address information to the sender. By restricting access to particular classes of persons/entities, the person can effectively prevent receipt of junk mail, other unsolicited mail, telemarketing calls and the like.

In a financial context, providing anonymous identification of a person enables the person to purchase goods and/or services from a merchant without ever transmitting to the merchant information, such as the person's credit card number, or even the person's name,

that could be intercepted and/or usurped and used in subsequent or additional unauthorized transactions or for other undesired purposes. Enabling anonymous identification may be particularly advantageous in an unsecured environment, such as the Internet, where it has been found to be relatively trivial to intercept such credit card information.

5 In a medical context, the USR system, in addition to enabling a person seeking medical treatment to identify themselves, may be configured to provide insurance data, medical history data, and other appropriate medical information to a medical provider, once that medical provider has been established as an authorized recipient. The USR system may also contain links to other databases containing portions of the patient's medical records, for
10 example x-rays, MRI pictures, dental records, glasses, prescriptions, etc.

 Access to the USR system may be by smart card, such as a SecurID™ card, or any other secure access device. The technology enabling the USR system may be physically embodied as a separate identification device such as a smart ID card, or may be incorporated into another electronic device, such as a cell phone, pager, wrist watch, computer, personal
15 digital assistant such as a Palm Pilot™, key fob, or other commonly available electronic device. The identity of the user possessing the identifying device may be verified at the point of use via any combination of a memorized PIN number or code, biometric identification such as a fingerprint, voice print, signature, iris or facial scan, or DNA analysis, or any other
20 method of identifying the person possessing the device. If desired, the identifying device may also be provided with a picture of the person authorized to use the device to enhance security.

 The USR system may be useful for numerous other identification purposes. For example, the USR anonymous identification may serve as a library card, a phone card, a health club card, a professional association membership card, a parking access card, a key for
25 access to one's home, office, car, etc. or any one of a host of similar identification/verification and/or access functions. Additionally, equipment code information may be stored in the USR system and distributed under the user's control and at the user's discretion, to maintain personal property or public property in an operative state.

30

BRIEF DESCRIPTION OF DRAWINGS

This invention is pointed out with particularity in the appended claims. The above and further advantages of this invention may be better understood by referring to the following description when taken in conjunction with the accompanying drawings. The accompanying drawings are not intended to be drawn to scale. In the drawings, each identical or nearly identical component that is illustrated in various figures is represented by a like numeral. For purposes of clarity, not every component may be labeled in every drawing. In the drawings:

Fig. 1 is a functional block diagram of a computer system configured to implement the universal secure registry (“USR”), including a USR database, according to one embodiment of the invention;

Fig. 2 is a functional block diagram of a first embodiment of a networked environment including the computer system of Fig. 1;

Fig. 3 is a functional block diagram of an entry of a database forming the USR database of Fig. 1;

Fig. 4 is a functional block diagram of a second embodiment of a networked environment including the computer system of Fig. 1;

Fig. 5 is a flow chart illustrating steps in a process of inputting data into the USR database;

Fig. 6 is a flow chart illustrating steps in a process of retrieving data from the USR database;

Fig. 7 is a flow chart illustrating a first protocol for purchasing goods from a merchant via the USR database without transmitting credit card information to the merchant;

Fig. 8 is a flow chart illustrating a second protocol for purchasing goods from a merchant via the USR database without transmitting credit card information to the merchant;

Fig. 9 is a flow chart illustrating a protocol for purchasing goods from a merchant via the USR database by validating the user’s check;

Fig. 10 is a flow chart illustrating a protocol for purchasing goods from an on-line merchant via the USR database without transmitting credit card information to the on-line merchant, and enabling the on-line merchant to ship the goods to a virtual address;

Fig. 11 is a flow chart illustrating a protocol for shipping goods to a virtual address via the USR database;

Fig. 12 is a flow chart illustrating a protocol for telephoning a virtual phone number via the USR database;

5 Fig. 13 is a flow chart illustrating a protocol for identifying a person via the USR database;

Fig. 14 is a flow chart illustrating a protocol for identifying a person to a policeman via the USR database;

10 Fig. 15 is a flow chart illustrating a protocol for providing information to an authorized recipient of the information via the USR database;

Fig. 16 is a flow chart illustrating a protocol for providing application information to an authorized recipient of the information via the USR database; and

15 Fig. 17 is a functional block diagram of an embodiment configured to use information in the USR system to activate or keep active property secured through the USR system.

DETAILED DESCRIPTION

This invention is not limited in its application to the details of construction and the arrangement of components set forth in the following description or illustrated in the drawings. The invention is capable of other embodiments and of being practiced or of being
20 carried out in various ways. Also, the phraseology and terminology used herein is for the purpose of description and should not be regarded as limiting. The use of “including,” “comprising,” or “having,” “containing”, “involving”, and variations thereof herein, is meant to encompass the items listed thereafter and equivalents thereof as well as additional items.

25 In one embodiment, an information system is formed as a computer program running on a computer or group of computers configured to provide a universal secure registry (USR) system. The computer, in this instance, may be configured to run autonomously (without the intervention of a human operator), or may require intervention or approval for all, a selected subset, or particular classes of transactions. The invention is not limited to the disclosed
30 embodiments, and may take on many different forms depending on the particular requirements of the information system, the type of information being exchanged, and the

type of computer equipment employed. An information system according to this invention, may optionally, but need not necessarily, perform functions additional to those described herein, and the invention is not limited to a computer system performing solely the described functions.

5 In the embodiment shown in Fig. 1, a computer system 10 for implementing a USR system according to the invention includes at least one main unit 12 connected to a wide area network, such as the Internet, via a communications port 14. The main unit 12 may include one or more processors (CPU 16) running USR software 18 configured to implement the USR system functionality discussed in greater detail below. The CPU 16 may be connected
10 to a memory system including one or more memory devices, such as a random access memory system RAM 20, a read only memory system ROM 22, and one or more databases 24. In the illustrated embodiment, the database 24 contains a universal secure registry database. The invention is not limited to this particular manner of storing the USR database. Rather, the USR database may be included in any aspect of the memory system, such as in
15 RAM 20, ROM 22 or disc and may also be separately stored on one or more dedicated data servers.

 The computer system may be a general purpose computer system which is programmable using a computer programming language, such as C, C++, Java, or other language, such as a scripting language or even assembly language. The computer system
20 may also be specially programmed, special purpose hardware, an application specific integrated circuit (ASIC) or a hybrid system including both special purpose components and programmed general purpose components.

 In a general purpose computer system, the processor is typically a commercially available microprocessor, such as Pentium series processor available from Intel, or other
25 similar commercially available device. Such a microprocessor executes a program called an operating system, such as UNIX, Linux, Windows NT, Windows 95, 98, or 2000, or any other commercially available operating system, which controls the execution of other computer programs and provides scheduling, debugging, input/output control, accounting, compilation, storage assignment, data management, memory management, communication
30 control and related services, and many other functions. The processor and operating system

defines a computer platform for which application programs in high-level programming languages are written.

The database 24 may be any kind of database, including a relational database, object-oriented database, unstructured database, or other database. Example relational databases
5 include Oracle 81 from Oracle Corporation of Redwood City, California; Informix Dynamic Server from Informix Software, Inc. of Menlo Park, California; DB2 from International Business Machines of Armonk, New York; and Access from Microsoft Corporation of Redmond, Washington. An example object-oriented database is ObjectStore from Object Design of Burlington, Massachusetts. An example of an unstructured database is Notes from
10 the Lotus Corporation, of Cambridge, Massachusetts. A database also may be constructed using a flat file system, for example by using files with character-delimited fields, such as in early versions of dBASE, now known as Visual dBASE from Inprise Corp. of Scotts Valley, California, formerly Borland International Corp.

The main unit 12 may optionally include or be connected to an user interface 26
15 containing, for example, one or more input and output devices to enable an operator to interface with the USR system 10. Illustrative input devices include a keyboard, keypad, track ball, mouse, pen and tablet, communication device, and data input devices such as voice and other audio and video capture devices. Illustrative output devices include cathode ray tube (CRT) displays, liquid crystal displays (LCD) and other video output devices, printers,
20 communication devices such as modems, storage devices such as a disk or tape, and audio or video output devices. Optionally, the user interface 26 may be omitted, in which case the operator may communicate with the USR system 10 in a networked fashion via the communication port 14. It should be understood that the invention is not limited to any particular manner of interfacing an operator with the USR system.

25 It also should be understood that the invention is not limited to a particular computer platform, particular processor, or particular high-level programming language. Additionally, the computer system may be a multiprocessor computer system or may include multiple computers connected over a computer network. It further should be understood that each module or step shown in the accompanying figures and the substeps or subparts shown in the
30 remaining figures may correspond to separate modules of a computer program, or may be separate computer programs. Such modules may be operable on separate computers. The

data produced by these components may be stored in a memory system or transmitted between computer systems.

Such a system may be implemented in software, hardware, or firmware, or any combination thereof. The various elements of the information system disclosed herein, either
5 individually or in combination, may be implemented as a computer program product, such as
USR software 18, tangibly embodied in a machine-readable storage device for execution by
the computer processor 16. Various steps of the process may be performed by the computer
processor 16 executing the program 18 tangibly embodied on a computer-readable medium to
perform functions by operating on input and generating output. Computer programming
10 languages suitable for implementing such a system include procedural programming
languages, object-oriented programming languages, and combinations of the two.

As shown in Fig. 2, the computer system 10 may be connected to a plurality of
interface centers 27 over a wide area network 28. The wide area network 28 may be formed
from a plurality of dedicated connections between the interface centers 27 and the computer
15 system 10, or may take place, in whole or in part, over a public network such as the Internet.
Communication between the interface centers 27 and the computer system 10 may take place
according to any protocol, such as TCP/IP, ftp, OFX, or XML, and may include any desired
level of interaction between the interface centers 27 and the computer system 10. To enhance
security, especially where communication takes place over a publicly accessible network
20 such as the Internet, communications facilitating or relating to transmission of data from/to
the USR database 24 or the computer system 10 may be encrypted using an encryption
algorithm, such as PGP, DES, or other conventional symmetric or asymmetric encryption
algorithm.

In one embodiment, the USR system 10 or USR database 24 may be able to
25 authenticate its identity to a user or other entity accessing the system by providing an
appropriate code which may be displayed on the user's smart card, for example a SecurID[™]
card or its equivalent, or other code generator, for example a single use code generator, being
employed by the user. A comparison by the user or the code generator between the provided
number and an expected number can validate, to the user (or other entity) or the code
30 generator, that communication is with the database and not an imposter.

The database 24 shown in Fig. 1 has a USR database containing entries related to persons 1-n. The data in the USR database may also be segregated, as shown in Fig. 4, according to data type to enable individual computer modules to handle discrete applications on discrete data types. Segregating the data, as illustrated in Fig. 4, may make access to the database more robust by enabling portions of the data in the USR database 24 to be accessible even when it is necessary to perform maintenance on a portion of the database. However, storing the data in the USR database 24 according to the scheme illustrated in Fig. 1 may make it easier for a user of the database to make changes to multiple types of data simultaneously or in a single session. There are advantages and disadvantages to each data structure, and the invention is not limited to a particular manner of organizing the data within the database 24, data structures other than the two shown also being possible.

As shown in Fig. 3, each entry 30 in the database 24 may contain multiple types of information. For example, in the embodiment shown in Fig. 3, the entry contains validation information 32, access information 34, publicly available information 36, address information 38, credit card and other financial information. 40, medical information 42, job application information 44, and tax information 46. The invention is not limited to a USR containing entries with all of this information or only this particular information, as any information on a person or other entity such as a company, institution, etc. may be stored in USR database 24.

If the database information is split between multiple databases, each database will typically include at least the validation and access information to enable the USR software to correlate a validation attempt with a verified validation, and to enable the USR software to determine access privileges to the requested data. Alternatively, databases may be linked to permit information not in a main USR database to be retrieved, with validation/identification for all databases accessed being done at the USR system.

In Fig. 3, the validation information is information about the user of the database to whom the data pertains and is to be used by the USR software 18 to validate that the person attempting to access the information is the person to whom the data pertains or is otherwise authorized to receive it. The validation information may be any type of information that will reliably authenticate the identity of the individual.

In one embodiment, the user of the database will carry a SecurID™ card available from RSA Security, formerly Security Dynamics Technologies, Inc., of Cambridge, MA.

Use of this card enables secure access to the USR database without requiring the user to transmit any personal information. Specifically, to access the USR database, the card retrieves a secret user code and/or time varying value from memory and obtains from the user a secret personal identification code. The card mathematically combines these three numbers
5 using a predetermined algorithm to generate a one-time nonpredictable code which is transmitted to the computer system 10. The computer system, specifically USR software 18, utilizes the received one-time nonpredictable code to determine if the user is authorized access to the USR database and grants access to the USR database if the user is determined to be authorized. The verification information 32 in the database entry in the embodiment of the
10 invention illustrated in Fig. 3 contains information to enable the USR software 18 to validate the user using such a card in this manner.

Alternative types of identification cards or tokens may likewise be used. For example, other smart cards may be used which generate non-predictable single use codes, which may or may not be time varying, or other access code generators may be used. An
15 algorithm generating such non-predictable codes may also be programmed onto a processor on a smart card or other computing device, such as a cell phone, pager, ID badge, wrist watch, computer, personal digital assistant, key fob, or other commonly available electronic device. For convenience, the term “electronic ID device” will be used generically to refer to any type of electronic device that may be used to obtain access to the USR database.

20 Likewise, various types of biometric information may be stored in the verification area of the database entry to enable the identity of the user possessing the identifying device to be verified at the point of use. Examples of the type of biometric information that may be used in this situation includes a personal identification number (PIN), fingerprint, voice print, signature, iris or facial scan, or DNA analysis. If desired, the verifying section of the
25 database may contain a picture to be transmitted back to the person seeking to validate the device to ensure the person using the device is the correct person. Optionally, the identifying device itself may also be provided with a picture of the person authorized to use the card to provide a facial confirmation of the person’s right to use the card.

In Fig. 3, the Access information 34 is provided to enable different levels of security
30 to attach to different types of information stored in the entry 30 in the USR database 14. For example, the person may desire that their address information be made available only to

certain classes of people, for example colleagues, friends, family, Federal Express, U.P.S., and the U.S. mail service. The names or universal identifiers for those selected individuals, companies, organizations and/or agencies may be entered into appropriate fields in the Access information to specify to the USR software 18 those individuals to whom the address
5 information may be released. Likewise, access fields may be specified for the other types of information. For example, the individual may specify that only particular individuals and/or companies have access to the credit card and other financial information 40, medical information 42, job application information 44 and tax information 46. Additionally, the individual may specify that no one have access to that information unless the individual
10 participates in the transaction (see Fig. 6).

As shown in Fig. 1, the USR software 18 contains algorithms for execution by the CPU 16 that enables the CPU 16 to perform the methods and functions of the USR software described below in connection with Figs. 5-16. The USR software 18, in this embodiment, performs all functions associated with validating an electronic ID card. If desired, a separate
15 validation software module may be provided to validate electronic ID devices outside of a firewall segregating the validation information from other user information.

The algorithms comprising the USR software 18 may be used to implement, in one exemplary embodiment, a USR system configured to enable selected information to be disseminated to selected individuals in a secure and dynamic fashion. This information may
20 be used for numerous purposes, several of which are set forth below and discussed in greater detail in connection with Figs. 5-16.

For example, the USR system may be used to identify the person, enable the person to be contacted by telephone or mail anonymously, enable the person to be contacted by telephone or by mail without revealing the person's telephone number or present location,
25 enable the person to purchase items over the Internet or in a store without revealing to the merchant any personal identification information or credit card information, enable the person to complete a job application without completing a job application form, enable the police to discern the person's identity and any outstanding warrants on the individual, and numerous other uses. The invention is not limited to these several enumerated uses, but
30 rather extends to any use of the USR database. The methods of using the USR database 24 will now be discussed in connection with Figs. 5-16.

Fig. 5 illustrates a method of training the USR database 24. As shown in Fig. 5, the USR software 18 first validates the person's identification (500). The initial validation of the person's identification (500) may take place at the point of sale of an electronic ID device (for example, a smart card). This may be done in any conventional manner, such as by
5 requiring the person to show a government issued identification card, passport, birth certificate, etc. Once the person's electronic ID device has been issued and initially validated, the validation process proceeds as discussed above.

After the validation process (500), the USR software 18 determines if the person has rights to enter data into the system (502). This step enables the system to charge persons for
10 maintaining information in the USR database 24. For example, the USR software 18 may poll a database of current accounts or a database of accounts that are currently in default to determine if the person has paid the access fee to enter data into the database. A similar account status inquiry process may be performed by the USR software 18 in connection with each of the other methods set forth in Figs. 6-16. If the person is not authorized to enter data
15 into the USR database 24, the person is notified of the status of their account and the process returns (512) to wait for further input from another person. Alternatively, a person may be permitted to enter some classes of data into the system and update such classes of data at no charge, with a fee possibly being required for other classes of data, for example medical records. This would facilitate a more robust database.

20 If the person is authorized, the USR software 18 then enables the person to enter basic personal data into the USR database 24 (504). Optionally, personal data may be one class of data the USR software 18 allows the person to enter into the USR database 18 regardless of account status, i.e., for free.

The USR software 18 will then check to see if the person has additional rights to enter
25 additional data (506), such as data to be entered into one of the other categories of data in Fig. 3. Optionally, this step of checking the person's rights to enter data (506) may be combined with the initial check (502). If the person does not have rights to enter any further data, the USR software 18 notifies the user and returns (512).

If the USR software 18 determines that the person has the right to enter additional
30 data into the USR database 24, the person is prompted through the use of appropriate prompts, provided with forms, and otherwise enabled to enter advanced personal data into the

USR database 24 (508). For each type of data entered, the person is asked to specify the type of access restrictions and/or whom should be allowed to access the advanced personal data (510). When the person has completed entering data into the database, the process returns (512) and commits the data to the database.

5 In the situation where only one person has access to enter and/or modify data for a given person in the database, there should be no conflict with committing data to the database. If, however, multiple people have access to a given account to modify data, the database may perform an integrity check to ensure the absence of conflict in the data before committing the new data to the database.

10 Enabling access to the information in the database will be explained in greater detail in connection with Fig. 6. As shown in Fig. 6, the database will generally allow anyone to access basic personal data on anyone without performing any authorization check (600).

 If information beyond that specified in the basic personal information area is requested, the USR software 18 queries whether the requestor has the right to access the type of requested data (602). The process of determining the requestor's rights (602) typically involves validating the requestor's identity and correlating the identity, the requested information and the access information 34 provided by the person to the USR database during the training process described above with respect to Fig. 5.

 If the USR software 18 determines that the requestor has rights to access the type of requested data (604), the USR software 18 instructs the USR database 24 to enable access to the type of requested data (606). The actual step of enabling access to the type of requested data may involve multiple steps of formulating a database query, querying the USR database 24, retrieving the results, assembling the results into a user friendly or user readable format, and transmitting the information to the user.

25 If the USR software 18 determines that the requestor does not have the appropriate rights to access the type of requested data (604), the USR software 18 checks to see if the person is participating in the transaction (608). Checking to see if the person is participating in the transaction enables the user to authorize access to the requested data in real time. For example, a person may wish to participate in a transaction to give a potential employer one-
30 time access to job application information 44 (see Fig. 3). If the person is not participating in

the transaction, the USR software 18 determines that the requestor is not authorized to have access to the requested data, notifies the requestor of this determination, and ends (610).

If the person is participating in the transaction (608), however, the USR software 18 validates the person's identity (612) and enables the person to change access rights to the data (614). If the USR software 18 is not able to validate the person's identity, the USR software 18 refuses to allow the person to update the database, notifies the person and/or requestor of this determination, and returns (610).

It is also possible that a person may be required to grant access to certain data, for example financial data such as account numbers, under duress. The system may provide the person with the ability to safely signal this when accessing the system by using a selected access code or by making a known modification to the access code provided by the electronic ID device. On receiving such code, the system would take appropriate steps to protect the person, including for example alerting the police, tracking the person's location to the extent possible, providing traceable data, and the like.

Once the person has had the opportunity to change access rights to the data (614), the USR software 18 again checks to see if the requestor has rights to access the type of requested data (616). Although step 616 may seem redundant, given the fact that the person is participating in the transaction and has just previously changed access rights to the database to enable the requestor to have access to the data, step 616 is actually useful at preventing a different type of fraud. Specifically, the requestor may not be forthright with the person regarding the type of information they are requesting. If step 616 were omitted, the USR software 18 may inadvertently allow access to an unauthorized type of information in the situation where the requestor has surreptitiously requested multiple types of data.

If the USR software 18 determines that the requestor has rights to the type of data requested (616), it causes the USR database to enable access to the type of requested data (606). Otherwise, it notifies the requestor of the decision to deny access to the requested data and returns (610).

Various applications of the USR database 24 and USR software 18 will now be discussed in connection with Figs. 7-16. These applications are merely exemplary of the types of applications enabled by the USR software 18 and USR database 24, and the invention is not limited to these particular applications.

Figure 7 illustrates one embodiment of a method of using the USR software 18 and USR database 24 to purchase goods or services from a merchant without revealing to the merchant account information relating to the person's bank or credit card.

As shown in Fig. 7, when a user initiates a purchase (700), the user enters a secret code in the user's electronic ID device (702) to cause the ID device to generate a onetime code or other appropriate code, and presents the electronic ID device with the code to the merchant or otherwise presents the code to the merchant. The merchant transmits to the credit card company (1) the code from the electronic ID device, (2) the store number, (3) the amount of the purchase (704), and the time of receipt of the code. The credit card company takes this information and passes the code from the electronic ID device to the USR software 18 (706). The USR software 18 determines if the code is valid, or was valid at the time offered, and if valid accesses the user's credit card information and transmits the appropriate credit card number to the credit card company (708). While the link between the USR system and the credit card system is a secure link, there is always a danger that the link may be penetrated and credit card numbers obtained. This may be avoided by instead transmitting, on approval, a multidigit public ID code for the credit card holder which the credit card company can map to the correct credit card number. Even if the link is violated, the public ID code is of no value and the secure link prevents this code from being improperly sent to the credit card company. The credit card company checks the credit worthiness of the user and declines the card or debits the user's account in accordance with its standard transaction processing system (710). The credit card company then notifies the merchant of the result of the transaction (712). In this embodiment, the user has been able to purchase goods or services from a merchant without ever providing to the merchant the credit card number. Since the electronic ID device generates a time variant code or otherwise generates a code that can for example only be used for a single transaction, the merchant retains no information from the transaction that may be fraudulently used in subsequent transactions.

Another embodiment of a system for facilitating purchase of goods or services without providing financial information to the merchant is set forth in Fig. 8. In Fig. 8, like Fig. 7, the user initiates a purchase (800), enters a secret code in the electronic ID device (802) and presents the resultant code to the merchant. The merchant, in this embodiment, transmits to the USR software 18, (1) the code from the electronic ID, (2) the store number,

and (3) the amount of the purchase (804). The USR software 18 determines if the code is valid (806) and, if valid, accesses from the USR database 24 the user's credit card information (808). The USR software then transmits to the credit card company (1) the credit card number, (2) the store number, and (3) the amount of purchase (808). The information in
5 this embodiment transmitted to the credit card company is intended to be in a format recognizable to the credit card company. Accordingly, the invention is not limited to transferring from the USR system 10 to the credit card company the enumerated information, but rather encompasses any transfer of information that will enable the use of the USR system 10 to appear transparent to the credit card company.

10 The credit card company then processes the transaction in a standard fashion, such as by checking the credit worthiness of the person, declining the card or debiting the user's account and transferring money to the merchant's account (810). The credit card company then notifies the USR system 10 the result of the transaction (812) and the USR software 18 in turn notifies the merchant of the result of the transaction (814).

15 In this embodiment, like the embodiment of Fig. 7, the user can use the USR system 10 to purchase goods or services from a merchant without providing the merchant with the user's credit card number. In the embodiment of Fig. 8, the interposition of the USR system 10 between the merchant and the credit card company is transparent to the credit card company and thus requires no or minimal cooperation from the credit card company to
20 implement.

Fig. 9 illustrates one embodiment of a method of using the USR system 10 to verify funds when using a check to purchase goods or services from a merchant. In the embodiment of Fig. 9, the user initiates a purchase and writes a check to the merchant (900). The check may be a conventional check containing identifying information, or may be a check bearing a
25 unique serial number and no identifying information to enable the check to be used anonymously.

In either situation, the user enters a secret code into the electronic ID card and presents the resulting code to the merchant along with the check (902). The merchant transmits to the USR software 18 (1) the code from the electronic ID card, (2) the store
30 number, and (3) the amount of the purchase (904). Where the check is an anonymous check, the merchant also transmits to the USR software 18 the check number.

The USR software 18 then determines if the code from the electronic ID is valid (906), and if valid accesses the user's bank information and transmits to the bank: (1) the user's bank account number, (2) the store number, and (3) the amount of the purchase (908). Optionally, the USR software 18 may additionally inform the bank of the check number.

5 The bank polls its own database to determine if there are sufficient funds in the user's account (910) and notifies the USR software 18 of the result (912). The USR software 18 then, in turn, notifies the merchant of the result of the verification (914).

10 This check verification system may take place over an unsecured connection between the merchant and the USR system 10 since the user's bank account information is not sent over the connection between the merchant and the USR system 10. Moreover, where an anonymous check is used, the merchant is not even provided with the person's name or account information in written form. This provides additional security against unauthorized persons writing subsequent checks.

15 The check verification system may be conducted over a telephone network, such as by having the merchant call a toll free number, or over a network connection such as over the Internet.

20 Fig. 10 illustrates a method of conducting a transaction with a merchant without requiring the user to provide to the merchant the user's name, address, or other identifying information, while enabling the merchant to ship the goods to the user. This may be beneficially employed, for example, in connection with transactions that take place between remote parties in a networked environment, such as the Internet.

25 As shown in Fig. 10, the user initiates an anonymous purchase by entering a secret code into the electronic ID device and transmitting the result to the on-line merchant (1000). The merchant transmits this information to the USR software 18, along with the store number and the amount of the purchase (1002). Optionally, the merchant may provide the store number and purchase price to the user and the user may send this information directly to the USR software 18 along with the code from the electronic ID. Where the number from the electronic ID device is a time varying number, the merchant may also need to input the time the number was received. Alternatively, the electronic ID device may encode or encrypt the
30 time with the number, the USR software being able to extract time when receiving the number from the merchant. This may not be required where the time varying number varies

slowly, for example changing every hour rather than every minute as for some existing such devices.

In either event, the USR software 18 determines if the code is valid (1004) and, if valid, accesses the user's credit card information from the USR database 24 (1006). The
5 USR software 18 then contacts the user's credit card company, as described above in connection with Fig. 8 (1008) and notifies the USR software 18 of the result (1000).

If the user's credit is declined, the USR software 18 notifies the on-line merchant and the transaction is terminated (1012). If the user's credit is honored, the USR software 18 polls the USR database 24 for the user's address and/or address code (1014). Address codes
10 are discussed below in greater detail with reference to Fig. 11. The merchant then packages the goods into a parcel, labels the parcel with the appropriate address and/or address code and ships the parcel to the user (1016). Having the USR system 10 provide the address and/or address code to the on-line merchant enables the user to purchase items in a networked
15 sale.

Fig. 11 illustrates a use of the USR database 24 to deliver mail to a user without requiring the user to provide address information to the sender. This may be useful in many contexts. For example, the user may wish that the address information be known only by the post office. In this instance, using the USR database 24 according to the method of the
20 invention described below, will enable the user to receive parcels without requiring the user to provide the merchant with the address information. Additionally, the user's address may change, temporarily, permanently, or frequently. Enabling the sender to send mail by entering a code instead of an address enables the post office to effectively deliver the coded mail to the corresponding address regardless of the frequency with which the address changes
25 or the duration in which the address will remain valid.

In Fig. 11, the user provides an address code on a public area of the USR database 24 that is available to all persons to see (1100). This code may for example be six alpha characters, which should be adequate for currently anticipated system populations. Optionally, the user may provide this code directly to a merchant or other person desirous of
30 sending the person one or more parcels.

The user also provides address information to the address information area 38 of the user's entry in the USR database 24 (1102). Access to the address information 38 is restricted by a rule or other appropriate entry in the access information 34 of the user's entry to only permit mail, parcel or other material delivery services, such as the US mail, UPS and
5 Fed Ex to access the address information.

When someone wishes to have a parcel or other items delivered to the user, the sender retrieves the user's address code from the USR database 24 or otherwise receives the address code from the user, and prints the address code on the parcel (1104).

The delivery service accesses the USR software 18, validates its identity, and queries
10 the USR database 24 for address information corresponding to the address code (1106). The USR database 24 retrieves the appropriate address data and provides the address information to the delivery service. The delivery service then either prints out an address label, prints a machine readable bar code to be attached to the package, or correlates an entry in a delivery database between the address code and the user address (1110). The delivery service then
15 uses this retrieved information to deliver the package to the user while never supplying the merchant with the user's permanent or temporary address. A user may also assure that mail, parcels, etc. are delivered to a current location by providing only a single notice to the USR system, regardless of how frequently the person moves. The person can also automatically provide for address changes where the person moves according to a known schedule. Thus,
20 deliveries to be made on a weekday could be directed to one address and deliveries on a weekend to another address; or deliveries during winter months to one address and during summer months to a different address.

Fig. 12 illustrates a method of enabling a person to telephone a user of the USR system 10 without providing the user's telephone number to the person. In the embodiment
25 illustrated in Fig. 12, the user provides a telephone code on the publicly available area of his entry on the USR database 24 (1200). This code may be assigned by the USR software 18 or made up by the user. The user also provides the USR database 24 with actual telephone information to enable the USR system 10 to connect callers with the user (1202).

The person wishing to telephone the user of the USR system 10 calls a telephone
30 number and enters the telephone code of the user (1204). The USR software 18, optionally, may require the person to identify themselves to see if they are authorized to call the user.

Assuming that the person is authorized to call the person, or if no authorization check is performed, the USR connects the person to the telephone number in the USR database 24 without providing the person with the telephone number.

5 Enabling the user to specify the telephone number may be advantageous for many reasons. First, the user may frequently be switching between telephone coverage areas and may wish to be reachable at all times. Simply by instructing the USR database 24 to connect incoming telephone calls to one of a myriad of numbers will facilitate connecting the incoming calls to, for example, the user's cell phone, work phone, pager, car phone or home phone, without necessitating the user to provide all these numbers to the caller. A similar
10 system may be implemented for facsimile transmissions, e-mails or other communications.

The user also may have predefined rules to enable telephone calls to follow a set pattern. For example, the user may desire to receive telephone calls only from family members during the night time at home, may wish to have all incoming calls routed to a car phone during commuting hours, and may wish to have all incoming calls routed to a cell
15 phone during lunch. These time dependent rules may and/or caller specific rules may be entered into the USR database to specify accessibility and connectivity of incoming telephone calls.

The publicly available address code and telephone code and any other codes may be the same, or may be different, there being some advantages to having a single code usable for
20 all such applications for each person on the system. The codes could be accessible through a variety of media including telephone and the internet. Where two or more people on the system have the same name, which will frequently be the case, additional publicly available biographical data may be provided with the name to assure that the right code is selected. The system may similarly be used to provide public keys for use in a public key/private key
25 encryption system, to provide other public codes for an individual or to provide other public information. Access to such information would typically be unrestricted.

Where the system is used to provide public keys, the public code used to obtain the key, or possibly the public key itself, may be used as above to obtain the e-mail address, telephone number or the like for the person to whom the message is being sent, and the USR
30 system may also be used to perform the encryption. When the recipient receives the message, he decrypts it using the recipient's private key in standard fashion, including decrypting

the name of the sender. However, this does not necessarily verify the sender and such verification may be desirable for important messages, particularly ones involving large financial transactions. The USR system may accomplish such verification by also storing private keys for people in the system. The sender first authenticates himself to the system, and the system then adds a second signature to the message which is encrypted with the sender's private key. The receiving party deencrypts this signature with the sender's public key. Since the system only sends such signatures for authenticated users, the message is thus verified.

Fig. 13 illustrates a general method of using the USR database 24 to authenticate a user's identification. This may be used in connection with any of the other methods disclosed herein to ensure that the electronic ID device has not been stolen and/or hacked by an unauthorized holder.

Specifically, in the embodiment illustrated in Fig. 13, the user attempts to prove identification to a validator, such as to prove that the possessor of the electronic ID device is of sufficient age to purchase alcohol (1300). In connection with this attempt, the user enters a secret code into the electronic ID (1302). The validator transmits to the USR software 18 the code from the electronic ID (1304). If the USR software 18 determines that the code is valid (1306), it accesses the user's photograph, age information, or any other desired information, and transmits that information to the validator (1308). By transmitting back to the validator a picture of the person to whom the electronic ID card was issued, the validator can ensure that the person using the electronic ID card is the proper person. Likewise, the validator can ensure, based on the information provided by the USR system 10, that the person is as old as the person claims to be.

A specific embodiment of this identification validation procedure is illustrated in Fig. 14. In Fig. 14, a policeman takes the place of the validator. In this scenario, however, instead of simply transmitting to the policeman a validation of the user's identity, such as their picture, the policeman may also receive additional information, such as the user's police records, records of any arrests, outstanding warrants, and other similar information that may be of use to the policeman when determining how to handle a particular individual.

Fig. 15 illustrates a process for enabling the user to provide specific information to a party, such as medical staff in an emergency room. As shown in Fig. 15, if the user desires to

provide information to a party (1500), the user enters a secret code in the electronic ID device and provides the electronic ID code to the party (1502). The party transmits to the USR software 18 the ID code and the party code (1504). The party code may be a code from for example an electronic device which identifies the party, may be a status code which identifies
5 the class of users to which the party belongs, for example policeman, emergency room personnel, doctor, etc. or may be a combination of both, the status code for example being encrypted into the ID code. The USR software 18 determines if the code is valid (1506), accesses the user's information in the USR database 24 and transmits available information to the party (1508). In this scenario, the user may be provided with a plurality of different codes
10 to enter into the electronic ID device depending on the type of information to be released to the party. For example, the user's basic code may be 1234. The fifth digit of the electronic code may specify the type of information to be provided, i.e., 1 = address information, 2 = medical information; 3 = telephone information, 4 = job application information, etc. Using multiple codes eliminates any ambiguity about the authority provided by the user to the party,
15 but requires the user to remember additional information.

The above assumes the user is able to provide an ID code when the information is required. However, in for example an emergency room situation, the user may not be in a position to provide the ID code, but would still want medical records provided. The release authorization for certain portions of the user's database could therefore specify that the
20 information be released to certain class or classes of individuals and the USR system would release such information to individuals or organizations based only on status code. Thus, the status code of an emergency room could alone trigger release of medical data.

Fig. 16 illustrates one embodiment of a method of using the USR database 24 to complete a standard application, such as a job application or an application to rent an
25 apartment. This embodiment is a specific example of the more generic method of enabling a party to retrieve information discussed above with respect to Fig. 15. In Fig. 16, however, the party may be provided with the opportunity to provide a form to the USR software 18, the fields of which may be automatically completed with information from the job application information section of the USR database 24.

30 As can be seen from the above, many of the users of the USR system are organizations or agencies such as carriers (post office, UPS, FedEx), communication

companies, law enforcement organizations, hospitals and other medical facilities and the like. Each of these organizations can be provided with specialized software either on a disc or other suitable media or electronically, for example over the internet, which performs a number of functions, for example automatically generating status codes for data access
5 requests, controlling information received, and formatting data received in response to a request in a desired way. This can result in an access request from such organization for a given user causing all data on the user required to complete the form being retrieved and presented to the organization in the format of their form. A user may also authorize an organization for which a form has been completed using the USR system to receive updates,
10 either in response to a request from the organization or at selected intervals, for example once a year, so as to maintain information in the forms current. Since the user will be providing information to the system on a regular basis, this is a relatively easy and painless way for the user to maintain current information with many organizations the user deals with.

Another potential use of the system is to permit a person to be located where only
15 limited biographical information on the person is known. Users of the USR system wishing to participate in this feature could be cued to provide non-confidential biographical data when they come on the system or at any time thereafter when they decide to participate. They can also indicate whether they wish their name given out in response to such an inquiry or to merely be alerted to an inquiry which might involve them and information on the requester.
20 A person seeking to find another person or group of people can input appropriate biographical data, for example members of 1975 Harvard University hockey team, or information of a person's last known address plus school information, etc. The system will then provide a list of persons who meet the listed criteria from which the person making the inquiry can hopefully find the person they are looking for.

25 In the above application and others, when a person is located, the person may request that only the person's address code or general access code (i.e. a single code which is used to get current address, telephone, e-mail, etc. information) be provided when the person is located. This can further protect the individual from undesired contacts.

Fig. 17 illustrates another embodiment of the invention. As shown in Fig. 17, the
30 USR system 10 may be used to secure expensive personal equipment, such as stereos, televisions, laptop computers, cellular telephones, cars, boats, and other items of value to a

person. In this embodiment, each item to be secured using the USR system is provided with a USR timer chip imbedded in the electronics. If the USR timer chip is not provided with a code within a predefined period of time, for example every 30 days, the equipment is deactivated. Thus, for example, a television, mobile phone, laptop computer, automobile,
5 heavy equipment, weapon or facility may be provided with a security chip having an internal timer that must be reset before expiration by provision of a particular code. When reset does not occur, the timer will disable the electronic device or other device using any one of a number of known disablement methods. Exemplary codes may be transmitted in the same manner as beeper signals are conventionally transmitted or may be transmitted to wired
10 devices over the Internet or other public network.

The USR system 10 may be advantageously employed to automatically provide the secured property with the necessary codes at appropriate intervals, unless instructed by the user of the USR system 10 to cease doing so. Alternatively, the USR system 10 may require participation by the user prior to sending out the activation codes.

15 In this embodiment, the user may provide to the USR system 10, information indicative of the codes to be transmitted, timing information, and automation information -- i.e., whether the codes should be sent automatically or should require user intervention. Optionally, where the user opts to require user intervention, the USR system 10 may notify the user of the upcoming deadline via e-mail or another method.

20 This system may be useful to secure sensitive equipment other than personal equipment as well, such as military equipment, public equipment, school equipment and any other equipment that is subject to theft.

It should be understood that various changes and modifications of the embodiments shown in the drawings and described in the specification may be made within the spirit and
25 scope of the present invention. Accordingly, it is intended that all matter contained in the above description and shown in the accompanying drawings be interpreted in an illustrative and not in a limiting sense. The invention is limited only as defined in the following claims and the equivalents thereto.

What is claimed is:

30

CLAIMS

1. A secure registry system for providing information to a service provider to enable the service provider to provide services to entities with secure data stored in the secure registry system, comprising:
- 5 a database including secure data for each entity and a multicharacter code for each entity having secure data in the secure registry system, the multicharacter code being mapped to the secure data; and
- a processor configured to receive the multicharacter code for the entity on whose behalf services are to be provided, configured to map the multicharacter code to information required by the service provider in order to provide the services, to provide the information to one of the service provider to perform the services or to a third party to enable a transaction without providing the information to the service provider.
- 10
- 15
2. The system of claim 1, wherein the multicharacter code is a secret code of the entity.
3. The system of claim 1, wherein the multicharacter code is provided via the entity via a secure electronic transmission device.
- 20
4. The system of claim 1, wherein the multicharacter code is encrypted and transmitted by the entity, and the system is configured to decrypt the multicharacter code with a public key of the entity.
- 25
5. The system as claimed in claim 1, wherein said service provider provides delivery services, wherein the information is an address to which an item is to be delivered for the entity, wherein the system receives the multicharacter code and the system uses the multicharacter code to obtain the appropriate address for delivery of the item.
- 30

6. The system as claimed in claim 1, wherein said provider provides telephone services, wherein the information is a current telephone number for the entity, wherein the system receives the multicharacter code and the system provides the current telephone number of the entity.

5

7. The system as claimed in claim 6, wherein the database comprises a plurality of rules and the current telephone number is one of a plurality of numbers to be provided based upon the plurality of rules.

10 8. The secure registry system as claimed in claim 1, wherein the system is configured to enable the service provider to perform the service without disclosing the secure data to the service provider.

15 9. The secure registry system as claimed in claim 1, wherein the information is credit card information regarding the entity, and wherein the processor is configured to provide the credit card information based upon the multicharacter code of the entity to enable a transaction.

20 10. The system as claimed in claim 9, wherein the system is configured to receive an approval of the credit card transaction without providing the credit card number of the entity to the service provider.

25 11. The system as claimed in claim 1, wherein the information is bank card information regarding the entity, and wherein the processor is configured to provide the bank card information to enable a transaction based upon the multicharacter code of the entity.

30 12. The system as claimed in claim 11, wherein the system is configured to provide an approval of the bank card transaction without providing the bank card number of the entity to the service provider.

13. The system as claimed in claim 1, wherein the information is personal identification information regarding the entity.

5 14. The system as claimed in claim 13, wherein the personal identification information comprises a photograph of the entity.

15. The system as claimed in claim 1, wherein the information is email address information regarding the entity.

10

16. A method for providing a service to entities who have secure data stored in a secure registry in which each entity is identified by a multicharacter code, the method comprising:

15 receiving the multicharacter code for an entity on whose behalf the services are to be provided;

mapping the multicharacter code to information required by the service provider in order to provide the services; and

using the corresponding information to perform the service.

20 17. The method of claim 16, wherein the act of using the corresponding information to perform the service comprises one of providing the information to one of the service provider to perform the services or to a third party to enable a transaction without providing the information to the service provider.

25 18. The method of claim 16, wherein the act of receiving the multicharacter code comprises receiving a secret multicharacter code which is secret to the entity.

19. The method of claim 16, wherein the act of receiving the multicharacter code comprises receiving the secret code which has been transmitted by via a secure electronic transmission device.

5 20. The method of claim 16, wherein the act of receiving the multicharacter code comprises receiving an encrypted multicharacter code and the method further comprises decrypting the encrypted multicharacter code.

10 21. The method as claimed in claim 16, wherein the service provider provides delivery services, the information is an address to which an item is to be delivered for the entity, the provider receives an item to be delivered and the address for delivery of the item.

15 22. The method as claimed in claim 16, wherein the service provider provides telephone service, the information is a telephone number for the entity, and the service provider connects a requestor to the telephone number of the entity.

20 23. The method as claimed in claim 16, wherein the acts of mapping the multicharacter code and using the information to perform the services comprises not providing the information to the provider of services.

25 24. The method as claimed in claim 16, wherein the act of using the information to perform the services comprises using credit card information about the entity to enable a transaction.

 25. The method as claimed in claim 24, wherein the act of using the information comprises receiving a validation or denial of the credit card transaction without providing the credit card number of the entity to the service provider.

26. The method as claimed in claim 16, wherein the act of using the information to perform the services comprises using bank card information about the entity to enable a transaction.

5 27. The method as claimed in claim 26, wherein the act of using the information comprises receiving a validation or denial of the bank card transaction without providing the bank card number of the entity to the service provider.

10 28. The method as claimed in claim 16, wherein the act of mapping the multicharacter code to information required by the service provider comprises mapping the multicharacter code into personal identification information about the entity.

15 29. The method as claimed in claim 28, wherein the personal identification information comprises a photograph of the entity.

30. The method as claimed in claim 16, wherein the information to comprises an email address information about the entity.

ABSTRACT

A secure registry system and method for the use thereof are provided which permits secure access to a database containing selected data on a plurality of entities, at least portions of which database has restricted access. Mechanisms are provided
5 for controlling access to restricted access portions of the database are provided, such access being determined by at least one of the identity of the requesting entity and the entity's status. A multicharacter public code may be provided which the system can map to provide permit delivery of items, complete telephone calls and perform other functions for entities. The system may also be utilized to locate an individual based
10 on limited biological data. Organizations utilizing the system may have custom software facilitating their access and use of the system.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	W0537-700620
		Application Number	
Title of Invention	UNIVERSAL SECURE REGISTRY		
The application data sheet is part of the provisional or nonprovisional application for which it is being submitted. The following form contains the bibliographic data arranged in a format specified by the United States Patent and Trademark Office as outlined in 37 CFR 1.76. This document may be completed electronically and submitted to the Office in electronic format using the Electronic Filing System (EFS) or the document may be printed and included in a paper filed application.			

Secrecy Order 37 CFR 5.2

- Portions or all of the application associated with this Application Data Sheet may fall under a Secrecy Order pursuant to 37 CFR 5.2 (Paper filers only. Applications that fall under Secrecy Order may not be filed electronically.)

Applicant Information:

Applicant 1					Remove
Applicant Authority <input checked="" type="radio"/> Inventor		<input type="radio"/> Legal Representative under 35 U.S.C. 117		<input type="radio"/> Party of Interest under 35 U.S.C. 118	
Prefix	Given Name	Middle Name	Family Name	Suffix	
	Kenneth	P.	Weiss		
Residence Information (Select One) <input checked="" type="radio"/> US Residency <input type="radio"/> Non US Residency <input type="radio"/> Active US Military Service					
City	Newton	State/Province	MA	Country of Residence ⁱ	US
Citizenship under 37 CFR 1.41(b) ⁱ		US			
Mailing Address of Applicant:					
Address 1	59 Sargent Street				
Address 2					
City	Newton	State/Province	MA		
Postal Code	02458	Country ⁱ	US		
All Inventors Must Be Listed - Additional Inventor Information blocks may be generated within this form by selecting the Add button.					Add

Correspondence Information:

Enter either Customer Number or complete the Correspondence Information section below. For further information see 37 CFR 1.33(a).			
<input type="checkbox"/> An Address is being provided for the correspondence information of this application.			
Customer Number	37462		
Email Address		Add Email	Remove Email

Application Information:

Title of the Invention	UNIVERSAL SECURE REGISTRY		
Attorney Docket Number	W0537-700620	Small Entity Status Claimed	<input checked="" type="checkbox"/>
Application Type	Nonprovisional		
Subject Matter	Utility		
Suggested Class (if any)		Sub Class (if any)	
Suggested Technology Center (if any)			
Total Number of Drawing Sheets (if any)	14	Suggested Figure for Publication (if any)	1

Application Data Sheet 37 CFR 1.76	Attorney Docket Number	W0537-700620
	Application Number	
Title of Invention	UNIVERSAL SECURE REGISTRY	

Publication Information:	
<input type="checkbox"/>	Request Early Publication (Fee required at time of Request 37 CFR 1.219)
<input type="checkbox"/>	Request Not to Publish. I hereby request that the attached application not be published under 35 U.S.C. 122(b) and certify that the invention disclosed in the attached application has not been and will not be the subject of an application filed in another country, or under a multilateral agreement, that requires publication at eighteen months after filing.

Representative Information:

Representative information should be provided for all practitioners having a power of attorney in the application. Providing this information in the Application Data Sheet does not constitute a power of attorney in the application (see 37 CFR 1.32). Enter either Customer Number or complete the Representative Name section below. If both sections are completed the Customer Number will be used for the Representative Information during processing.			
Please Select One:	<input checked="" type="radio"/> Customer Number	<input type="radio"/> US Patent Practitioner	<input type="radio"/> US Representative (37 CFR 11.9)
Customer Number	37462		

Domestic Priority Information:

This section allows for the applicant to claim benefit under 35 U.S.C. 119(e), 120, 121, or 365(c). Providing this information in the application data sheet constitutes the specific reference required by 35 U.S.C. 119(e) or 120, and 37 CFR 1.78(a)(2) or CFR 1.78(a)(4), and need not otherwise be made part of the specification.					
Prior Application Status	Patented		<input type="button" value="Remove"/>		
Application Number	Continuity Type	Prior Application Number	Filing Date (YYYY-MM-DD)	Patent Number	Issue Date (YYYY-MM-DD)
	Continuation of	09810703	2001-03-16	7237117	2007-06-26
Additional Domestic Priority Data may be generated within this form by selecting the Add button.					<input type="button" value="Add"/>

Foreign Priority Information:

This section allows for the applicant to claim benefit of foreign priority and to identify any prior foreign application for which priority is not claimed. Providing this information in the application data sheet constitutes the claim for priority as required by 35 U.S.C. 119(b) and 37 CFR 1.55(a).			
			<input type="button" value="Remove"/>
Application Number	Country ⁱ	Parent Filing Date (YYYY-MM-DD)	Priority Claimed
			<input type="radio"/> Yes <input checked="" type="radio"/> No
Additional Foreign Priority Data may be generated within this form by selecting the Add button.			<input type="button" value="Add"/>

Assignee Information:

Providing this information in the application data sheet does not substitute for compliance with any requirement of part 3 of Title 37 of the CFR to have an assignment recorded in the Office.	
Assignee 1	<input type="button" value="Remove"/>
If the Assignee is an Organization check here. <input type="checkbox"/>	

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Application Data Sheet 37 CFR 1.76		Attorney Docket Number	W0537-700620	
		Application Number		
Title of Invention	UNIVERSAL SECURE REGISTRY			

Prefix	Given Name	Middle Name	Family Name	Suffix

Mailing Address Information:

Address 1				
Address 2				
City		State/Province		
Country i		Postal Code		
Phone Number		Fax Number		
Email Address				

Additional Assignee Data may be generated within this form by selecting the **Add** button.

Signature:

A signature of the applicant or representative is required in accordance with 37 CFR 1.33 and 10.18. Please see 37 CFR 1.4(d) for the form of the signature.

Signature	/John N. Anastasi/		Date (YYYY-MM-DD)	2007-06-26	
First Name	John	Last Name	Anastasi	Registration Number	37765

This collection of information is required by 37 CFR 1.76. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 23 minutes to complete, including gathering, preparing, and submitting the completed application data sheet form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

DECLARATION FOR PATENT APPLICATION

As a below named inventor, I hereby declare that:

My residence, post office address and citizenship are as stated below next to my name.

I believe I am the original, first and sole inventor (if only one name is listed below) or an original, first and joint inventor (if plural names are listed below) of the subject matter which is claimed and for which a patent is sought on the invention entitled

UNIVERSAL SECURE REGISTRY

the specification of which is attached hereto unless the following is checked:

was filed on March 16, 2001, as Application No. 09/810,703, bearing attorney docket No. W0537/7006.

I hereby state that I have reviewed and understand the contents of the above identified specification, including the claims, as amended by any amendment referred to above.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, Code of Federal Regulations, §1.56.

I hereby claim the benefit under Title 35, United States Code, §119(e) of any United States provisional application(s) listed below:

_____ (Application Number)	_____ (filing date)
_____ (Application Number)	_____ (filing date)

I hereby claim the benefit under Title 35, United States Code, §120 of any United States application(s), or §365(c) of any PCT International application(s) designating the United States of America listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in the prior United States or PCT International application in the manner provided by the first paragraph of Title 35, United States Code, §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations, §1.56 which became available between the filing date of the prior application and the national or PCT International filing date of this application:

_____ (Application No.)	_____ (filing date)	_____ (status-patented, pending, abandoned)
_____ (Application No.)	_____ (filing date)	_____ (status-patented, pending, abandoned)

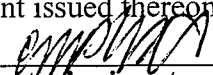
PCT International Applications designating the United States:

(PCT Appl. No.)	(U.S. Ser. No.)	(PCT filing date)	(status-patented,pending,abandoned)		
Robert M. Abrahamsen	40,886	Jason M. Honeyman	31,624	Randy J. Pritzker	35,986
Eric Amundsen	46,518	Robert E. Hunt	39,231	Robert E. Rigby, Jr.	36,904
John N. Anastasi	37,765	Ronald J. Kransdorf	20,004	Edward J. Russavage	43,069
Ilan Barzilay	46,540	Peter C. Lando	34,654	Stanley Sacks	19,900
Gary S. Engelson	35,128	M. Brad Lawrence	47,210	Christopher S. Schultz	37,929
Neil P. Ferraro	39,188	Helen C. Lockhart	39,248	Robert A. Skrivanek, Jr.	41,316
Thomas G. Field III	45,596	Matthew B. Lowrie	38,228	Alan W. Steele	45,128
Stephen R. Finch	42,534	William R. McClellan	29,409	Mark Steinberg	40,829
Edward R. Gates	31,616	Daniel P. McLoughlin	46,066	Joseph Teja, Jr.	45,157
Richard F. Giunta	36,149	James H. Morris	34,681	John R. Van Amsterdam	40,212
Lawrence M. Green	29,384	M. Lawrence Oliverio	30,915	Robert H. Walat	46,324
George L. Greenfield	17,756	Timothy J. Oyer	36,628	Kristin D. Wheeler	43,583
James M. Hanifin, Jr.	39,213	Edward F. Perlman	28,105	Lisa E. Winsor	44,405
Therese A. Hendricks	30,389	Elizabeth R. Plumer	36,637	David Wolf	17,528
Steven J. Henry	27,900	Michael J. Pomianek	46,190	Douglas R. Wolf	36,971

Address all telephone calls to Ronald P. Kransdorf at telephone no. (617) 720-3500. Address all correspondence to:

Ronald P. Kransdorf
 c/o Wolf, Greenfield & Sacks, P.C.,
 Federal Reserve Plaza
 600 Atlantic Avenue
 Boston, MA 02210-2211

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

	<u>12/18/01</u>
Inventor's signature	Date
Full name first inventor:	Kenneth P. Weiss
Citizenship:	USA
Residence:	59 Sargent Street Newton, MA 02158
Post Office Address:	59 Sargent Street Newton, MA 02158

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		
	Filing Date		2007-06-26
	First Named Inventor	Kenneth P. Weiss	
	Art Unit		
	Examiner Name	Not Yet Known	
	Attorney Docket Number	W0537-700620	

U.S.PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1	5664109		1997-09-02	Johnson, et al.		
	2	5813006		1998-09-22	Polnerow et al.		
	3	6073106		2000-06-06	Rozen et al.		
	4	62532002	B1	2001-06-26	Gilmour		
	5	6253203	B1	2001-06-26	O'Flaherty et al.		
	6	6260039	B1	2001-07-10	Schneck et al.		
	7	6308203	B1	2001-10-23	Itabashi et al.		
	8	6393421	B1	2002-05-21	Paglin		

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		
Filing Date		2007-06-26
First Named Inventor	Kenneth P. Weiss	
Art Unit		
Examiner Name	Not Yet Known	
Attorney Docket Number	W0537-700620	

	9	6516315	B1	2003-02-04	Gupta	
	10	6546005	B1	2003-04-08	Berkley et al	
	11	6581059	B1	2003-07-17	Barrett et al.	
	12	6640211	B1	2003-10-28	Holden	
	13	6658400	B2	2003-12-02	Perell et al.	
	14	6845448	B1	2005-01-18	Chaganti et al.	
	15	6941271	B1	2005-09-06	Soong	
	16	5058161		1991-10-15	Weiss	
	17	5168520		1992-12-01	Weiss	
	18	5657388		1997-08-12	Weiss	
	19	6393421		2002-05-21	Paglin	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		
Filing Date		2007-06-26
First Named Inventor	Kenneth P. Weiss	
Art Unit		
Examiner Name	Not Yet Known	
Attorney Docket Number	W0537-700620	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20010032100	A1	2001-10-18	Mahmud et al.	
	2	20020046061	A1	2002-04-18	Wright et al.	
	3	20040117215	A1	2004-06-17	Marchosky	
	4	20030226041		2003-12-04	Glennard Palmer, Richardson	
	5	20040133787		2004-07-08	Doughty, Ralph O.	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² j	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							<input type="checkbox"/>

If you wish to add additional Foreign Patent Document citation information please click the Add button.

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number			
	Filing Date		2007-06-26	
	First Named Inventor	Kenneth P. Weiss		
	Art Unit			
	Examiner Name	Not Yet Known		
	Attorney Docket Number	W0537-700620		

	1		<input type="checkbox"/>
--	---	--	--------------------------

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

***EXAMINER:** Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number			
	Filing Date		2007-06-26	
	First Named Inventor	Kenneth P. Weiss		
	Art Unit			
	Examiner Name	Not Yet Known		
	Attorney Docket Number	W0537-700620		

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/John N. Anastasi/	Date (YYYY-MM-DD)	2007-06-26
Name/Print	John N. Anastasi	Registration Number	37765

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:				
Filing Date:				
Title of Invention:	UNIVERSAL SECURE REGISTRY			
First Named Inventor/Applicant Name:	KENNETH P. WEISS			
Filer:	John N Anastasi/Fareesha Ali			
Attorney Docket Number:	W0537-700620			
Filed as Small Entity				
Utility Filing Fees				
Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Utility filing Fee (Electronic filing)	4011	1	75	75
Utility Search Fee	2111	1	250	250
Utility Examination Fee	2311	1	100	100
Pages:				
Claims:				
Claims in excess of 20	2202	10	25	250
Miscellaneous-Filing:				
Petition:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
Total in USD (\$)				675

Electronic Acknowledgement Receipt

EFS ID:	1912446
Application Number:	11768729
International Application Number:	
Confirmation Number:	3536
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	KENNETH P. WEISS
Customer Number:	37462
Filer:	John N Anastasi
Filer Authorized By:	
Attorney Docket Number:	W0537-700620
Receipt Date:	26-JUN-2007
Filing Date:	
Time Stamp:	17:48:10
Application Type:	Utility

Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	\$ 675
RAM confirmation Number	2590
Deposit Account	502762

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part /.zip	Pages (if appl.)
-----------------	----------------------	-----------	------------------	------------------	------------------

1	Drawings	806189_Figures.pdf	272531	no	14
Warnings:					
Information:					
2		809184_Application.pdf	156999	yes	32
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Specification		1	26	
	Claims		27	31	
	Abstract		32	32	
Warnings:					
Information:					
3	Application Data Sheet	809191_ADS.PDF	911941	no	4
Warnings:					
Information:					
4	Oath or Declaration filed	809210_Declaration.PDF	104655	no	2
Warnings:					
Information:					
5	Information Disclosure Statement (IDS) Filed	809211_IDS.PDF	1228492	no	6
Warnings:					
Information:					
6	Fee Worksheet (PTO-06)	fee-info.pdf	8473	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			2683091		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

6/26/07

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	11/768,729
---	-------------------

APPLICATION AS FILED – PART I			SMALL ENTITY		OTHER THAN SMALL ENTITY	
	(Column 1)	(Column 2)				
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	RATE (\$)	FEE (\$)
BASIC FEE (37 CFR 1.16(a), (b), or (c))				75		
SEARCH FEE (37 CFR 1.16(k), (l), or (m))				250		
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))				100		
TOTAL CLAIMS (37 CFR 1.16(i))	30	minus 20 =	X 25=	250	X 50=	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	2	minus 3 =	X 100=		X 200=	
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).					
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))			N/A		N/A	
			TOTAL	675	TOTAL	

* If the difference in column 1 is less than zero, enter "0" in column 2.

APPLICATION AS AMENDED – PART II					SMALL ENTITY		OTHER THAN SMALL ENTITY	
	(Column 1)	(Column 2)	(Column 3)					
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	*	Minus **	=	X =		X =	
	Independent (37 CFR 1.16(h))	*	Minus ***	=	X =		X =	
	Application Size Fee (37 CFR 1.16(s))				N/A		N/A	
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					TOTAL ADD'T FEE		TOTAL ADD'T FEE	

APPLICATION AS AMENDED – PART II					SMALL ENTITY		OTHER THAN SMALL ENTITY	
	(Column 1)	(Column 2)	(Column 3)					
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)
	Total (37 CFR 1.16(i))	*	Minus **	=	X =		X =	
	Independent (37 CFR 1.16(h))	*	Minus ***	=	X =		X =	
	Application Size Fee (37 CFR 1.16(s))				N/A		N/A	
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))					TOTAL ADD'T FEE		TOTAL ADD'T FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
 ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
 *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
 The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 7 columns: APPLICATION NUMBER, FILING or 371(c) DATE, GRP ART UNIT, FIL FEE REC'D, ATTY.DOCKET.NO, TOT CLAIMS, IND CLAIMS. Values: 11/768,729, 06/26/2007, 675, W0537-700620, 30, 2

CONFIRMATION NO. 3536

FILING RECEIPT

37462
LOWRIE, LANDO & ANASTASI
RIVERFRONT OFFICE
ONE MAIN STREET, ELEVENTH FLOOR
CAMBRIDGE, MA02142

Date Mailed: 07/30/2007

Receipt is acknowledged of this non-provisional patent application. The application will be taken up for examination in due course. Applicant will be notified as to the results of the examination. Any correspondence concerning the application must include the following identification information: the U.S. APPLICATION NUMBER, FILING DATE, NAME OF APPLICANT, and TITLE OF INVENTION. Fees transmitted by check or draft are subject to collection. Please verify the accuracy of the data presented on this receipt. If an error is noted on this Filing Receipt, please write to the Office of Initial Patent Examination's Filing Receipt Corrections. Please provide a copy of this Filing Receipt with the changes noted thereon. If you received a "Notice to File Missing Parts" for this application, please submit any corrections to this Filing Receipt with your reply to the Notice. When the USPTO processes the reply to the Notice, the USPTO will generate another Filing Receipt incorporating the requested corrections

Applicant(s)

Kenneth P. Weiss, Newton, MA;

Power of Attorney: None

Domestic Priority data as claimed by applicant

This application is a CON of 09/810,703 03/16/2001 PAT 7,237,117

Foreign Applications

If Required, Foreign Filing License Granted:

Projected Publication Date: To Be Determined - pending completion of Security Review

Non-Publication Request: No

Early Publication Request: No

** SMALL ENTITY **

Title

UNIVERSAL SECURE REGISTRY

Preliminary Class

PROTECTING YOUR INVENTION OUTSIDE THE UNITED STATES

Since the rights granted by a U.S. patent extend only throughout the territory of the United States and have

no effect in a foreign country, an inventor who wishes patent protection in another country must apply for a patent in a specific country or in regional patent offices. Applicants may wish to consider the filing of an international application under the Patent Cooperation Treaty (PCT). An international (PCT) application generally has the same effect as a regular national patent application in each PCT-member country. The PCT process **simplifies** the filing of patent applications on the same invention in member countries, but **does not result** in a grant of "an international patent" and does not eliminate the need of applicants to file additional documents and fees in countries where patent protection is desired.

Almost every country has its own patent law, and a person desiring a patent in a particular country must make an application for patent in that country in accordance with its particular laws. Since the laws of many countries differ in various respects from the patent law of the United States, applicants are advised to seek guidance from specific foreign countries to ensure that patent rights are not lost prematurely.

Applicants also are advised that in the case of inventions made in the United States, the Director of the USPTO must issue a license before applicants can apply for a patent in a foreign country. The filing of a U.S. patent application serves as a request for a foreign filing license. The application's filing receipt contains further information and guidance as to the status of applicant's license for foreign filing.

Applicants may wish to consult the USPTO booklet, "General Information Concerning Patents" (specifically, the section entitled "Treaties and Foreign Patents") for more information on timeframes and deadlines for filing foreign patent applications. The guide is available either by contacting the USPTO Contact Center at 800-786-9199, or it can be viewed on the USPTO website at <http://www.uspto.gov/web/offices/pac/doc/general/index.html>.

For information on preventing theft of your intellectual property (patents, trademarks and copyrights), you may wish to consult the U.S. Government website, <http://www.stopfakes.gov>. Part of a Department of Commerce initiative, this website includes self-help "toolkits" giving innovators guidance on how to protect intellectual property in specific countries such as China, Korea and Mexico. For questions regarding patent enforcement issues, applicants may call the U.S. Government hotline at 1-866-999-HALT (1-866-999-4158).

LICENSE FOR FOREIGN FILING UNDER

Title 35, United States Code, Section 184

Title 37, Code of Federal Regulations, 5.11 & 5.15

GRANTED

The applicant has been granted a license under 35 U.S.C. 184, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" followed by a date appears on this form. Such licenses are issued in all applications where the conditions for issuance of a license have been met, regardless of whether or not a license may be required as set forth in 37 CFR 5.15. The scope and limitations of this license are set forth in 37 CFR 5.15(a) unless an earlier license has been issued under 37 CFR 5.15(b). The license is subject to revocation upon written notification. The date indicated is the effective date of the license, unless an earlier license of similar scope has been granted under 37 CFR 5.13 or 5.14.

This license is to be retained by the licensee and may be used at any time on or after the effective date thereof unless it is revoked. This license is automatically transferred to any related applications(s) filed under 37 CFR 1.53(d). This license is not retroactive.

The grant of a license does not in any way lessen the responsibility of a licensee for the security of the subject matter as imposed by any Government contract or the provisions of existing laws relating to espionage and the national security or the export of technical data. Licensees should apprise themselves of current regulations especially with respect to certain countries, of other agencies, particularly the Office of Defense Trade Controls, Department of State (with respect to Arms, Munitions and Implements of War (22 CFR 121-128)); the Bureau of Industry and Security, Department of Commerce (15 CFR parts 730-774); the Office of Foreign Assets Control, Department of Treasury (31 CFR Parts 500+) and the Department of

Energy.

NOT GRANTED

No license under 35 U.S.C. 184 has been granted at this time, if the phrase "IF REQUIRED, FOREIGN FILING LICENSE GRANTED" DOES NOT appear on this form. Applicant may still petition for a license under 37 CFR 5.12, if a license is desired before the expiration of 6 months from the filing date of the application. If 6 months has lapsed from the filing date of this application and the licensee has not received any indication of a secrecy order under 35 U.S.C. 181, the licensee may foreign file the application pursuant to 37 CFR 5.15(b).

Clear
9/26/07

DEPARTMENT OF DEFENSE
ACCESS ACKNOWLEDGEMENT / SECRECY ORDER RECOMMENDATION
FOR PATENT APPLICATION

Application Serial No: DP11768729

Filing Date:

Date Referred: 07/19/2007

I hereby acknowledge that the Department of Defense reviewers has inspected this application in administration of 35 USC 181 on behalf of the Agencies/Commands specified below. DoD reviewers will not divulge any information from this application for any purpose other than administration of 35 USC 181.

Defense Agency	Recommendation	Reviewer Name	Date Reviewed
NSA	Secrecy Not Recommended	Robert Morelli	08/15/2007

<p><i>Type of Recommendations:</i> <i>SNR: Secrecy Not Recommended</i> <i>SR: Secrecy Recommended</i> <i>NC: No Comment</i></p>
--

Instructions to Reviewers:

1. All DoD personnel reviewing this application will be listed on this form regardless of whether they are making a secrecy order recommendation.
2. This form will be forwarded to USPTO once all assigned DoD entities have provided their secrecy order recommendation.

Time for Completion of Review:

Pursuant to 35 USC 184, the subject matter of this application may be filed in a foreign country for the purpose of filing a patent application without a license anytime after the expiration of six (6) months from filing date unless the application becomes the subject of a secrecy order.

<p><i>The USPTO publishes patent application at 18 months from the earliest claimed filing date. The USPTO will delay the publication of a patent application made available to a defense agency under 35 USC 181 until no earlier than 6 months from the filing date or 90 days from the date of referral to that agency. This application will be cleared for publication 6 months from the filing date or 90 days from the above Date Referred, whichever is later, unless a response is provided to the USPTO regarding the necessary recommendations as to the imposition of a secrecy order.</i></p>
--

<p>DoD Completion of Review: Final</p>

<p>Forwarded to USPTO: 08/16/2007 By: Luis Marrero</p>
--



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(c) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/768,729	06/26/2007	Kenneth P. Weiss	W0537-700620

CONFIRMATION NO. 3536

37462
LOWRIE, LANDO & ANASTASI
RIVERFRONT OFFICE
ONE MAIN STREET, ELEVENTH FLOOR
CAMBRIDGE, MA02142

Date Mailed. 09/27/2007

NOTICE OF NEW OR REVISED PROJECTED PUBLICATION DATE

The above-identified application has a new or revised projected publication date. The current projected publication date for this application is 01/03/2008. If this is a new projected publication date (there was no previous projected publication date), the application has been cleared by Licensing & Review or a secrecy order has been rescinded and the application is now in the publication queue.

If this is a revised projected publication date (one that is different from a previously communicated projected publication date), the publication date has been revised due to processing delays in the USPTO or the abandonment and subsequent revival of an application. The application is anticipated to be published on a date that is more than six weeks different from the originally-projected publication date.

More detailed publication information is available through the private side of Patent Application Information Retrieval (PAIR) System. The direct link to access PAIR is currently <http://pair.uspto.gov>. Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Questions relating to this Notice should be directed to the Office of Patent Publication at 1-888-786-0101.

PART 1 - ATTORNEY/APPLICANT COPY

Docket No.: W0537-700620

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Kenneth P. Weiss
Serial No: 11/768,729
Confirmation No: 3536
Filed: June 26, 2007
For: UNIVERSAL SECURE REGISTRY

Examiner: Not Yet Assigned
Art Unit: Not Yet Assigned

CERTIFICATE OF TRANSMISSION UNDER 37 C.F.R. §1.8(a)

The undersigned hereby certifies that this document is being electronically filed in accordance with § 1.6(a)(4), on the 27th day of December, 2007.

/John N. Anastasi/
John N. Anastasi

Commissioner for Patents
Alexandria, VA 22313-1450

PRELIMINARY AMENDMENT

Sir:

Please amend the above-identified application as indicated herein. Changes to the Specification are shown by strike through (for deleted matter) and underlining (for added matter).

Amendments to the Specification begin on page 2 of this paper.

Remarks begin on page 3 of this paper.

Amendments to the Specification

Please replace the paragraph beginning at page 1, line 4 with the following:

This application claims the benefit under 35 U.S.C. § 120 of U.S. Application Serial No. 09/810,703, filed on March 16, 2001 and issued on June 26, 2007 as Patent No. 7,237,117, which is herein incorporated by reference in its entirety.

REMARKS

In this Preliminary Amendment, the specification has been amended to correct a minor typographical error discovered. No new matter has been added. Applicant respectfully requests entry of this amendment.

CONCLUSION

In view of the foregoing amendments and remarks, reconsideration is respectfully requested. This application should now be in condition for allowance; a notice to this effect is respectfully requested. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicant's attorney at the telephone number listed below.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicants hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee that is not covered by the enclosed payment, please charge any deficiency to Deposit Account No. 50/2762, Ref. No.: W0537-700620.

Respectfully submitted,
Kenneth P. Weiss, et al., Applicants

By: /John N. Anastasi/
John N. Anastasi, Reg. No. 37,765
LOWRIE, LANDO & ANASTASI, LLP
One Main Street
Cambridge, Massachusetts 02142
United States of America
Telephone: 617-395-7001
Facsimile: 617-395-7070

Electronic Acknowledgement Receipt

EFS ID:	2643454
Application Number:	11768729
International Application Number:	
Confirmation Number:	3536
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Customer Number:	37462
Filer:	John N Anastasi
Filer Authorized By:	
Attorney Docket Number:	W0537-700620
Receipt Date:	27-DEC-2007
Filing Date:	26-JUN-2007
Time Stamp:	12:22:31
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1		816252_Preliminary_Amend ment.pdf	29692 bd3ea7311a5e0b9f8c21b2923dfddddd0 535e124d	yes	3

Multipart Description/PDF files in .zip description			
Document Description		Start	End
Preliminary Amendment		1	1
Specification		2	2
Applicant Arguments/Remarks Made in an Amendment		3	3

Warnings:

Information:

Total Files Size (in bytes):

29692

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 11/768,729	Filing Date 06/26/2007	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

APPLICATION AS FILED – PART I			OTHER THAN SMALL ENTITY				
	(Column 1)	(Column 2)	SMALL ENTITY <input checked="" type="checkbox"/>	OR			
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	OR	RATE (\$)	FEE (\$)
<input type="checkbox"/> BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>	N/A	N/A	N/A			N/A	
<input type="checkbox"/> SEARCH FEE <small>(37 CFR 1.16(k), (l), or (m))</small>	N/A	N/A	N/A			N/A	
<input type="checkbox"/> EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A	N/A			N/A	
TOTAL CLAIMS <small>(37 CFR 1.16(i))</small>	minus 20 =	*	X \$ =		OR	X \$ =	
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>	minus 3 =	*	X \$ =			X \$ =	
<input type="checkbox"/> APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.16(j))</small>							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY				
	(Column 1)	(Column 2)	(Column 3)		SMALL ENTITY	OR			
AMENDMENT	12/27/2007	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	* 30	Minus ** 30	= 0	X \$25 =	0	OR	X \$ =	
	Independent <small>(37 CFR 1.16(h))</small>	* 2	Minus *** 3	= 0	X \$105 =	0	OR	X \$ =	
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>								
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>						OR		
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

	(Column 1)	(Column 2)	(Column 3)		SMALL ENTITY	OR			
AMENDMENT	Total <small>(37 CFR 1.16(i))</small>	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	*	Minus	**	=	X \$ =		OR	X \$ =	
	Independent <small>(37 CFR 1.16(h))</small>	*	Minus	***	X \$ =		OR	X \$ =	
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>								
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>						OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
 ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
 *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

Legal Instrument Examiner:
 Deborah Scott

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



APPLICATION NUMBER	FILING OR 371(c) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/768,729	06/26/2007	Kenneth P. Weiss	W0537-700620

CONFIRMATION NO. 3536

37462
LOWRIE, LANDO & ANASTASI, LLP
ONE MAIN STREET, SUITE 1100
CAMBRIDGE, MA02142

Title: UNIVERSAL SECURE REGISTRY

Publication No. US-2008-0005576-A1

Publication Date: 01/03/2008

NOTICE OF PUBLICATION OF APPLICATION

The above-identified application will be electronically published as a patent application publication pursuant to 37 CFR 1.211, et seq. The patent application publication number and publication date are set forth above.

The publication may be accessed through the USPTO's publicly available Searchable Databases via the Internet at www.uspto.gov. The direct link to access the publication is currently <http://www.uspto.gov/patft/>.

The publication process established by the Office does not provide for mailing a copy of the publication to applicant. A copy of the publication may be obtained from the Office upon payment of the appropriate fee set forth in 37 CFR 1.19(a)(1). Orders for copies of patent application publications are handled by the USPTO's Office of Public Records. The Office of Public Records can be reached by telephone at (703) 308-9726 or (800) 972-6382, by facsimile at (703) 305-8759, by mail addressed to the United States Patent and Trademark Office, Office of Public Records, Alexandria, VA 22313-1450 or via the Internet.

In addition, information on the status of the application, including the mailing date of Office actions and the dates of receipt of correspondence filed in the Office, may also be accessed via the Internet through the Patent Electronic Business Center at www.uspto.gov using the public side of the Patent Application Information and Retrieval (PAIR) system. The direct link to access this status information is currently <http://pair.uspto.gov/>. Prior to publication, such status information is confidential and may only be obtained by applicant using the private side of PAIR.

Further assistance in electronically accessing the publication, or about PAIR, is available by calling the Patent Electronic Business Center at 1-866-217-9197.

Pre-Grant Publication Division, 703-605-4283

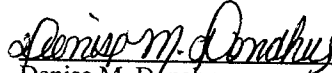
IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Kenneth P. Weiss
Serial No: 09/810,703
Confirmation No.: 7223
Filed: March 16, 2001
For: UNIVERSAL SECURE REGISTRY
Examiner: Not Yet Assigned
Art Unit: 2131

CERTIFICATE OF MAILING UNDER 37 CFR §1.8(a)

The undersigned hereby certifies that this document is being placed in the United States mail with first-class postage attached, addressed to Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on the 13th day of ~~October~~, 2003.

November


Denise M. Donahue

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

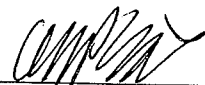
POWER OF ATTORNEY
(REVOCAION OF PRIOR POWERS)

As inventor of the above-identified application, all powers of attorney previously given are hereby revoked and the following attorneys and/or agents affiliated with the customer number below are hereby appointed to prosecute and transact all business in the Patent and Trademark Office connected therewith:

37462

Address all telephone calls to John N. Anastasi at telephone no. (617) 395-7000. Address all correspondence to:

John N. Anastasi
c/o Lowrie, Lando & Anastasi, LLP
Riverfront Office Park, One Main Street
Cambridge, MA 02142

By: 
Name: Kenneth P. Weiss

Electronic Acknowledgement Receipt

EFS ID:	2858036
Application Number:	11768729
International Application Number:	
Confirmation Number:	3536
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Customer Number:	37462
Filer:	John N Anastasi
Filer Authorized By:	
Attorney Docket Number:	W0537-700620
Receipt Date:	14-FEB-2008
Filing Date:	26-JUN-2007
Time Stamp:	19:12:55
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes) /Message Digest	Multi Part /.zip	Pages (if appl.)
1	Power of Attorney	W0537-700620_Power_of_A ttorney.pdf	36587 <small>aba9dbdc00514d7906b5cb96fc3720b0 4827626e</small>	no	1

Warnings:

Information:

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
11/768,729	06/26/2007	Kenneth P. Weiss	W0537-7006

CONFIRMATION NO. 3536

POA ACCEPTANCE LETTER

John N. Anastasi
c/o Lowrie, Lando & Anastasi, LLP
Riverfront Office Park, One Main Street
Cambridge, MA 02142



Date Mailed: 02/26/2008

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 02/14/2008.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/s/brahim/

Office of Initial Patent Examination (571) 272-4000 or 1-800-PTO-9199

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11768729
	Filing Date	2007-06-26
	First Named Inventor	Kenneth P. Weiss
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	W0537-700620

U.S. PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	
	1	4720860		1988-01-19	Weiss		
	2	4856062		1989-08-08	Weiss		
	3	4885778		1989-12-05	Weiss		
	4	4998279		1991-03-05	Weiss		
	5	5023908		1991-06-11	Weiss		
	6	5097505		1992-03-17	Weiss		
	7	5237614		1993-08-17	Weiss		
	8	5361062		1994-11-01	Weiss		

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	11768729
Filing Date	2007-06-26
First Named Inventor	Kenneth P. Weiss
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	W0537-700620

9	5367572		1994-11-22	Weiss	
10	5479512		1995-12-26	Weiss	
11	5485519		1996-01-16	Weiss	
12	5915023		1999-06-22	Bernstein	
13	6130621		2000-10-10	Weiss	
14	6253202		2001-06-26	Gilmour	
15	7237117		2007-06-26	Weiss	

If you wish to add additional U.S. Patent citation information please click the Add button.

[Add](#)

U.S.PATENT APPLICATION PUBLICATIONS

[Remove](#)

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

[Add](#)

FOREIGN PATENT DOCUMENTS

[Remove](#)

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		11768729	
	Filing Date		2007-06-26	
	First Named Inventor	Kenneth P. Weiss		
	Art Unit		N/A	
	Examiner Name	Not Yet Assigned		
	Attorney Docket Number		W0537-700620	

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² j	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							<input type="checkbox"/>

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1		<input type="checkbox"/>

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11768729
	Filing Date	2007-06-26
	First Named Inventor	Kenneth P. Weiss
	Art Unit	N/A
	Examiner Name	Not Yet Assigned
	Attorney Docket Number	W0537-700620

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/John N. Anastasi/	Date (YYYY-MM-DD)	2008-08-26
Name/Print	John N. Anastasi	Registration Number	37765

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	3841974
Application Number:	11768729
International Application Number:	
Confirmation Number:	3536
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Correspondence Address:	John N. Anastasi c/o Lowrie, Lando & Anastasi, LLP Riverfront Office Park, One Main Street - Cambridge MA 02142 US 6173957000 -
Filer:	John N Anastasi
Filer Authorized By:	
Attorney Docket Number:	W0537-7006
Receipt Date:	26-AUG-2008
Filing Date:	26-JUN-2007
Time Stamp:	16:25:09
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Information Disclosure Statement (IDS) Filed (SB/08)	W0537-700620_IDS_Form__SB_08a.pdf	574231 <small>ee9c187f7abcdb218c2747cca6622ae8d4568553</small>	no	5

Warnings:

Information:

Total Files Size (in bytes):	574231
-------------------------------------	--------

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/768,729	06/26/2007	Kenneth P. Weiss	W0537-7006	3536

7590 07/20/2009
John N. Anastasi
c/o Lowrie, Lando & Anastasi, LLP
Riverfront Office Park, One Main Street
Cambridge, MA 02142

EXAMINER

DADA, BEEMNET W

ART UNIT	PAPER NUMBER
----------	--------------

2435

MAIL DATE	DELIVERY MODE
-----------	---------------

07/20/2009

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

DETAILED ACTION

Claims 1-30 are presented for examination.

Information Disclosure Statement

The information disclosure statement (IDS) submitted on 06/26/2007 and 08/26/2008 have been considered. The submission is in compliance with the provisions of 37 CFR 1.97. Form PTO-1449 is signed and attached hereto.

Drawings

The drawings filed on June 26, 2007 are accepted.

Specification

The specification filed June 26, 2007 is accepted.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Art Unit: 2435

Claims 1-3, 5-19 and 21-30 are rejected under 35 U.S.C. 102(e) as being anticipated by Soong US 6,941,271 B1.

As per claim 1, Soong teaches a secure registry system for providing information to a service provider to enable the service provider to provide services to entities with secure data stored in the secure registry system, comprising:

a database including secure data for each entity and a multicharacter code for each entity having secure data in the secure registry system, the multicharacter code being mapped to the secure data [column 6, lines 33-44]; and

a processor configured to receive the multicharacter code for the entity on whose behalf services are to be provided, configured to map the multicharacter code to information required by the service provider in order to provide the services, to provide the information to one of the service provider to perform the services or to a third party to enable a transaction without providing the information to the service provider [column 6, lines 16-59].

As per claim 16, Soong teaches a method for providing a service to entities who have secure data stored in a secure registry in which each entity is identified by a multicharacter code, the method comprising:

receiving the multicharacter code for an entity on whose behalf the services are to be provided [column 6, lines 14-32] ;

mapping the multicharacter code to information required by the service provider in order to provide the services [column 6, lines 28-59]; and

using the corresponding information to perform the service [column 6, lines 28-59].

Art Unit: 2435

As per claims 2 and 18, Soong further teaches the system wherein the multicharacter code is a secret code of the entity [column 6, lines 14-32].

As per claims 3 and 19, Soong further teaches the system wherein the multicharacter code is provided via the entity via a secure electronic transmission device [column 6, lines 14-32].

As per claims 5 and 21, Soong further teaches the system wherein said service provider provides delivery services, wherein the information is an address to which an item is to be delivered for the entity, wherein the system receives the multicharacter code and the system uses the multicharacter code to obtain the appropriate address for delivery of the item [column 6, lines 28-59].

As per claims 6, 7 and 22, Soong further teaches the system wherein said provider provides telephone services, wherein the information is a current telephone number for the entity, wherein the system receives the multicharacter code and the system provides the current telephone number of the entity [column 6, lines 28-59].

As per claims 8 and 23, Soong further teaches the system wherein the system is configured to enable the service provider to perform the service without disclosing the secure data to the service provider [column 6, lines 28-59].

As per claims 9, 10, 24 and 25, Soong further teaches the system wherein the information is credit card information regarding the entity, and wherein the processor is

Art Unit: 2435

configured to provide the credit card information based upon the multicharacter code of the entity to enable a transaction [column 6, lines 28-59].

As per claims 11, 12, 26 and 27, Soong further teaches the system wherein the information is bank card information regarding the entity, and wherein the processor is configured to provide the bank card information to enable a transaction based upon the multicharacter code of the entity [column 6, lines 28-59].

As per claims 13, 14, 28 and 29, Soong further teaches the system wherein the information is personal identification information regarding the entity [column 6, lines 28-59].

As per claims 15 and 30, Soong further teaches the system wherein the information is email address information regarding the entity [column 6, lines 28-59].

As per claim 17, Soong further teaches the system wherein the act of using the corresponding information to perform the service comprises one of providing the information to one of the service provider to perform the services or to a third party to enable a transaction without providing the information to the service provider [column 6, lines 28-59].

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 4 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Soong US 6,941,271 B1 in view of Borgelt et al US 5,398,285 (hereinafter Borgelt).

As per claims 4 and 20, Soong teaches the system/method as indicated above. Soong is silent on the system wherein the multicharacter code is encrypted and transmitted by the entity, and the system is configured to decrypt the multicharacter code with a public key of the entity. In the same field of endeavor, Borgelt teaches a system wherein the multicharacter code is encrypted and transmitted by the entity, and the system is configured to decrypt the multicharacter code with a public key of the entity [see abstract]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Borgelt within the system of Soong in order to enhance the security of the system.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BEEMNET W. DADA whose telephone number is (571)272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2435

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Beemnet W Dada/
Primary Examiner, Art Unit 2435
July 16, 2009

Notice of References Cited	Application/Control No. 11/768,729	Applicant(s)/Patent Under Reexamination WEISS, KENNETH P.	
	Examiner BEEMNET W. DADA	Art Unit 2435	Page 1 of 1

U.S. PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A US-5,398,285	03-1995	Borgelt et al.	380/30
*	B US-6,941,271	09-2005	Soong, James W.	705/3
	C US-			
	D US-			
	E US-			
	F US-			
	G US-			
	H US-			
	I US-			
	J US-			
	K US-			
	L US-			
	M US-			


FOREIGN PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N				
	O				
	P				
	Q				
	R				
	S				
	T				

NON-PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)				
	U				
	V				
	W				
	X				

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims 	Application/Control No. 11768729	Applicant(s)/Patent Under Reexamination WEISS, KENNETH P.
	Examiner BEEMNET W DADA	Art Unit 2435

✓	Rejected
=	Allowed

-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

Claims renumbered in the same order as presented by applicant
 CPA
 T.D.
 R.1.47

CLAIM		DATE									
Final	Original	07/16/2009									
	1	✓									
	2	✓									
	3	✓									
	4	✓									
	5	✓									
	6	✓									
	7	✓									
	8	✓									
	9	✓									
	10	✓									
	11	✓									
	12	✓									
	13	✓									
	14	✓									
	15	✓									
	16	✓									
	17	✓									
	18	✓									
	19	✓									
	20	✓									
	21	✓									
	22	✓									
	23	✓									
	24	✓									
	25	✓									
	26	✓									
	27	✓									
	28	✓									
	29	✓									
	30	✓									

Receipt date: 06/26/2007

11768729, GAU: 2435

Approved for use through 09/30/2007. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		
	Filing Date		2007-06-26
	First Named Inventor	Kenneth P. Weiss	
	Art Unit		
	Examiner Name	Not Yet Known	
	Attorney Docket Number	W0537-700620	

U.S. PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	
	1	5664109		1997-09-02	Johnson, et al.		
	2	5813006		1998-09-22	Polnerow et al.		
	3	6073106		2000-06-06	Rozen et al.		
	4	62532002	B1	2001-06-26	Gilmour		
	5	6253203	B1	2001-06-26	O'Flaherty et al.		
	6	6260039	B1	2001-07-10	Schneck et al.		
	7	6308203	B1	2001-10-23	Itabashi et al.		
	8	6393421	B1	2002-05-21	Paglin		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BD/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		11768729 - GAU: 2435	
	Filing Date		2007-06-26	
	First Named Inventor	Kenneth P. Weiss		
	Art Unit			
	Examiner Name	Not Yet Known		
	Attorney Docket Number		W0537-700620	

	9	6516315	B1	2003-02-04	Gupta	
	10	6546005	B1	2003-04-08	Berkley et al	
	11	6581059	B1	2003-07-17	Barrett et al.	
	12	6640211	B1	2003-10-28	Holden	
	13	6658400	B2	2003-12-02	Perell et al.	
	14	6845448	B1	2005-01-18	Chaganti et al.	
	15	6941271	B1	2005-09-06	Soong	
	16	5058161		1991-10-15	Weiss	
	17	5168520		1992-12-01	Weiss	
	18	5657388		1997-08-12	Weiss	
	19	6393421		2002-05-21	Paglin	

Receipt date: 06/26/2007 INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		11768729 - GAU: 2435	
	Filing Date		2007-06-26	
	First Named Inventor	Kenneth P. Weiss		
	Art Unit			
	Examiner Name	Not Yet Known		
	Attorney Docket Number	W0537-700620		

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20010032100	A1	2001-10-18	Mahmud et al.	
	2	20020046061	A1	2002-04-18	Wright et al.	
	3	20040117215	A1	2004-06-17	Marchosky	
	4	20030226041		2003-12-04	Glennard Palmer, Richardson	
	5	20040133787		2004-07-08	Doughty, Ralph O.	

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² i	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							<input type="checkbox"/>

If you wish to add additional Foreign Patent Document citation information please click the Add button.

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		11768729 - GAU: 2435
	Filing Date		2007-06-26
	First Named Inventor	Kenneth P. Weiss	
	Art Unit		
	Examiner Name	Not Yet Known	
	Attorney Docket Number	W0537-700620	

	1		<input type="checkbox"/>
--	---	--	--------------------------

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Beemnet Dada/	Date Considered	07/16/2009
--------------------	----------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		11768729 - GAU: 2435
	Filing Date		2007-06-26
	First Named Inventor	Kenneth P. Weiss	
	Art Unit		
	Examiner Name	Not Yet Known	
	Attorney Docket Number	W0537-700620	

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/John N. Anastasi/	Date (YYYY-MM-DD)	2007-06-26
Name/Print	John N. Anastasi	Registration Number	37765

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	11768729
Filing Date	2007-06-26
First Named Inventor	Kenneth P. Weiss
Art Unit	N/A
Examiner Name	Not Yet Assigned
Attorney Docket Number	W0537-700620

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	4720860		1988-01-19	Weiss	
	2	4856062		1989-08-08	Weiss	
	3	4885778		1989-12-05	Weiss	
	4	4998279		1991-03-05	Weiss	
	5	5023908		1991-06-11	Weiss	
	6	5097505		1992-03-17	Weiss	
	7	5237614		1993-08-17	Weiss	
	8	5361062		1994-11-01	Weiss	

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		11768729	11768729 - GAU: 2435
	Filing Date		2007-06-26	
	First Named Inventor	Kenneth P. Weiss		
	Art Unit		N/A	
	Examiner Name	Not Yet Assigned		
	Attorney Docket Number		W0537-700620	

	9	5367572		1994-11-22	Weiss	
	10	5479512		1995-12-26	Weiss	
	11	5485519		1996-01-16	Weiss	
	12	5915023		1999-06-22	Bernstein	
	13	6130621		2000-10-10	Weiss	
	14	6253202		2001-06-26	Gilmour	
	15	7237117		2007-06-26	Weiss	

If you wish to add additional U.S. Patent citation information please click the Add button.

U.S.PATENT APPLICATION PUBLICATIONS

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Published Application citation information please click the Add button.

FOREIGN PATENT DOCUMENTS

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BD/

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		11768729	11768729 - GAU: 2435
	Filing Date		2007-06-26	
	First Named Inventor	Kenneth P. Weiss		
	Art Unit	N/A		
	Examiner Name	Not Yet Assigned		
	Attorney Docket Number	W0537-700620		

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² i	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1							<input type="checkbox"/>

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1		<input type="checkbox"/>

If you wish to add additional non-patent literature document citation information please click the Add button


EXAMINER SIGNATURE

Examiner Signature	/Beemnet Dada/	Date Considered	07/16/2009
--------------------	----------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BD/

Search Notes 	Application/Control No. 11768729	Applicant(s)/Patent Under Reexamination WEISS, KENNETH P.
	Examiner BEEMNET W DADA	Art Unit 2435

SEARCHED			
Class	Subclass	Date	Examiner
713	169, 182, 184	7/16/09	BD
707	9	7/16/09	BD

SEARCH NOTES		
Search Notes	Date	Examiner
East search	7/16/09	BD
IEEE, Google, Citeseer	7/16/09	BD
Inventor name search	7/16/09	BD

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

--	--


UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
 Address: COMMISSIONER FOR PATENTS
 P.O. Box 1450
 Alexandria, Virginia 22313-1450
 www.uspto.gov

BIB DATA SHEET
CONFIRMATION NO. 3536

SERIAL NUMBER	FILING or 371(c) DATE RULE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.		
11/768,729	06/26/2007	713	2435	W0537-7006		
APPLICANTS Kenneth P. Weiss, Newton, MA; ** CONTINUING DATA ***** This application is a CON of 09/810,703 03/16/2001 PAT 7,237,117 ** FOREIGN APPLICATIONS ***** ** IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** ** SMALL ENTITY **						
Foreign Priority claimed	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No	<input type="checkbox"/> Met after Allowance	STATE OR COUNTRY	SHEETS DRAWINGS	TOTAL CLAIMS	INDEPENDENT CLAIMS
35 USC 119(a-d) conditions met	<input type="checkbox"/> Yes <input type="checkbox"/> No	Initials	MA	14	30	2
Verified and Acknowledged	/BEE MNET W DADA/ Examiner's Signature					
ADDRESS John N. Anastasi c/o Lowrie, Lando & Anastasi, LLP Riverfront Office Park, One Main Street Cambridge, MA 02142 UNITED STATES						
TITLE UNIVERSAL SECURE REGISTRY						
FILING FEE RECEIVED 675	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:			<input type="checkbox"/> All Fees		
				<input type="checkbox"/> 1.16 Fees (Filing)		
				<input type="checkbox"/> 1.17 Fees (Processing Ext. of time)		
				<input type="checkbox"/> 1.18 Fees (Issue)		
				<input type="checkbox"/> Other _____		
			<input type="checkbox"/> Credit			

Docket No.: W0537-700620

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Kenneth P. Weiss
Serial No: 11/768,729
Confirmation No: 3536
Filed: June 26, 2007
For: UNIVERSAL SECURE REGISTRY

Examiner: Dada, Beemnet W.
Art Unit: 2435

CERTIFICATE OF TRANSMISSION UNDER 37 C.F.R. §1.8(a)

The undersigned hereby certifies that this document is being electronically filed in accordance with § 1.6(a)(4), on the 20th day of November, 2009.

/Robert V. Donahoe/
Robert V. Donahoe, Reg. No. 46,667

Commissioner for Patents

AMENDMENT

Sir:

In response to the Office Action mailed July 20, 2009, please amend the above-identified application as follows. Changes to the Claims are shown by strike through (for deleted matter) and underlining (for added matter).

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks begin on page 8 of this paper.

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

5

Listing of Claims:

1. (Currently Amended) A secure registry system for providing information to a service provider to enable the service provider to provide services to entities with
10 secure data stored in the secure registry system, comprising:
 - a database including secure data for each entity and a multicharacter code for each entity having secure data in the secure registry system, the multicharacter code being mapped to the secure data; and
 - a processor configured to receive, from the service provider, the
15 multicharacter code for the entity on whose behalf services are to be provided, configured to map the multicharacter code to information required ~~by the service provider in order~~ to provide the services where the information is unknown to the service provider, to provide the information ~~to one of the service provider to perform the services or~~ to a third party to enable a transaction without providing the
20 information to the service provider.
2. (Original) The system of claim 1, wherein the multicharacter code is a secret code of the entity.
- 25 3. (Currently Amended) The system of claim 1, wherein the multicharacter code is provided to the system via the entity via a secure electronic transmission device.
4. (Currently Amended) The system of claim 1, wherein the multicharacter code is encrypted and transmitted to the system by the entity, and the system is configured
30 to decrypt the multicharacter code with a public key of the entity.

5. (Currently Amended) The system as claimed in claim 1, wherein said service provider's service includes ~~provides~~ delivery-services, wherein the information is an address to which an item is to be delivered ~~to~~for the entity, wherein the system receives the multicharacter code and the system uses the multicharacter code to obtain
5 the appropriate address for delivery of the item by the third party.

6. (Canceled)

7. (Canceled)

10

8. (Currently Amended) The secure registry system as claimed in claim 1, wherein the information includes the secure data~~wherein the system is configured to enable the service provider to perform the service without disclosing the secure data to the service provider.~~

15

9. (Currently Amended) The secure registry system as claimed in claim 31[[1]], wherein the identity information includes credit card information regarding the entity, and wherein the processor is configured to provide the credit card information based upon the multicharacter code of the entity to enable the a-transaction.

20

10. (Original) The system as claimed in claim 9, wherein the system is configured to receive an approval of the credit card transaction without providing the credit card number of the entity to the service provider.

25

11. (Currently Amended) The system as claimed in claim 31, wherein the identity information includes bank card information regarding the entity, and wherein the processor is configured to provide the bank card information to enable the a transaction based upon the multicharacter code of the entity.

12. (Original) The system as claimed in claim 11, wherein the system is configured to provide an approval of the bank card transaction without providing the bank card number of the entity to the service provider.
- 5 13. (Currently Amended) The system as claimed in claim 31, wherein the information is personal identification information regarding the entity.
14. (Original) The system as claimed in claim 13, wherein the personal identification information comprises a photograph of the entity.
- 10 15. (Original) The system as claimed in claim 1, wherein the information is email address information regarding the entity.
16. (Currently Amended) A method for providing a service to entities who have
15 secure data stored in a secure registry in which each entity is identified by a multicharacter code, the service provided by a service provider, the method comprising:
- receiving the multicharacter code for an entity on whose behalf the services are to be provided;
- 20 mapping the multicharacter code to information required ~~by the service provider in order~~ to provide the services;
- providing the information to a third party without providing the information to the service provider; and
- 25 ~~using the corresponding~~ information to enable the service provider to provide ~~perform~~ the service without the service provider's knowledge of the information.
17. (Canceled)
- .

18. (Original) The method of claim 16, wherein the act of receiving the multicharacter code comprises receiving a secret multicharacter code which is secret to the entity.
- 5 19. (Original) The method of claim 16, wherein the act of receiving the multicharacter code comprises receiving the secret code which has been transmitted by via a secure electronic transmission device.
20. (Original) The method of claim 16, wherein the act of receiving the
10 multicharacter code comprises receiving an encrypted multicharacter code and the method further comprises decrypting the encrypted multicharacter code.
21. (Currently Amended) The method as claimed in claim 16, wherein the service provider's service includes provides delivery services, wherein the information is an
15 address to which an item is to be delivered for the entity, and wherein the third party the provider receives an item to be delivered and the address for delivery of the an
item provided by the service provider.
22. (Canceled)
- 20 23. (Canceled)
24. (Original) The method as claimed in claim 16, wherein the act of using the information to perform the services comprises using credit card information about the
25 entity to enable a transaction.
25. (Original) The method as claimed in claim 24, wherein the act of using the information comprises receiving a validation or denial of the credit card transaction without providing the credit card number of the entity to the service provider.
30

26. (Original) The method as claimed in claim 16, wherein the act of using the information to perform the services comprises using bank card information about the entity to enable a transaction.
- 5 27. (Original) The method as claimed in claim 26, wherein the act of using the information comprises receiving a validation or denial of the bank card transaction without providing the bank card number of the entity to the service provider.
28. (Currently Amended) The method as claimed in claim 16, wherein the act of
10 mapping the multicharacter code to information required by the service provider
comprises mapping the multicharacter code ~~into~~ to personal identification information
about the entity.
29. (Original) The method as claimed in claim 28, wherein the personal
15 identification information comprises a photograph of the entity.
30. (Original) The method as claimed in claim 16, wherein the information to
comprises an email address information about the entity.
- 20 31. (New) The system of claim 1, wherein the information includes identity
information concerning the entity.
32. (New) The method as claimed in claim 24, further comprising an act of
transmitting to the service provider one of an approval or a denial of the credit card
25 transaction without providing the credit card number of the entity to the service
provider.
33. (New) The system of claim 1, wherein the database is further configured to
associate biometric information with each entity having secure data in the secure
30 registry, respectively.

34. (New) The system of claim 33, wherein the processor is further configured to map the multicharacter code to biometric information associated with the entity on whose behalf the services are to be provided and to provide the biometric information to the service provider.
- 5
35. (New) The system of claim 34, wherein the biometric information includes an image of the entity on whose behalf the services are to be provided.
36. (New) The system of claim 34, wherein the multicharacter code comprises a
10 time-varying multicharacter code generated by a device associated with the entity on whose behalf services are to be provided.
37. (New) The method as claimed in claim 16, further comprising an act of
15 associating biometric information with each entity having secure data in the secure registry, respectively.
38. (New) The method of claim 37, further comprising acts of:
mapping the multicharacter code to biometric information associated with the
entity on whose behalf the services are to be provided; and
20 providing the biometric information to the service provider.
39. (New) The method of claim 38, wherein the biometric information includes
an image of the entity on whose behalf the services are to be provided.
- 25 40. (New) The method of claim 38, further comprising an act of generating a time-varying multicharacter code by a device associated with the entity on whose behalf the services are to be provided.

REMARKS

Claims 1-30 were previously pending in this application. By this amendment, Applicant is canceling claims 6, 7, 17, 22, and 23 without prejudice or disclaimer. Claims 1, 3-5, 8, 9, 11, 13, 16, 21 and 28 are amended herein. New claims 31-40 are added herein. As a result claims 1-5, 8-16, 18-21 and 24-40 are pending for examination with claims 1 and 16 being independent claims. No new matter has been added. Support for the amendments to the independent claims can be found at least, for example, in Figs. 7-10 and the associated description at pages 17-20 of the application as originally filed. Support for the new claims can be found at least, for example, at page 12, lines 20-28 and page 17, lines 5-26.

Rejections Under 35 U.S.C. §102

The Office Action rejects claims 1-3, 5-19 and 21-30 under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,941,271 B1 to Soong (hereinafter Soong). This rejection includes the rejection of independent claims 1 and 16.

Applicants respectfully assert that Soong does not anticipate independent claims 1 and 16, as amended herein. Claim 1 recites “a secure registry system for providing information to a service provider to enable the service provider to provide services to entities with secure data stored in the secure registry system, comprising ... a processor configured to receive, from the service provider, the multicharacter code for the entity on whose behalf services are to be provided, configured to map the multicharacter code to information required to provide the services where the information is unknown to the service provider, to provide the information to a third party to enable a transaction without providing the information to the service provider.” (Emphasis added.) Claim 16 recites a “method for providing a service to entities who have secure data stored in a secure registry in which each entity is identified by a multicharacter code, the service provided by a service provider, the method comprising: receiving the multicharacter code for an entity on whose behalf the services are to be provided; mapping the multicharacter code to information required to provide the services; providing the information to a third party without providing the information to the service provider; and using the information to enable the service provider to provide the service without the service provider’s knowledge of the information.” (Emphasis added.)

Soong describes a method for accessing component fields of a patient record where access to a site computer by authorized persons is provided through the use of login IDs and passwords. (Col. 6, lines 14-59.) User are allowed access to patient records, for example, when they provide the correct password. In each case, the user seeking access to a patient's records has knowledge of the information needed to login and gain access. *Id.* Accordingly, the mere description of login IDs and passwords does not describe either: a secure registry system for providing information to a service provider to enable the service provider to provide services to entities with secure data stored in the secure registry system, ... where the information is unknown to the service provider, to provide the information to a third party to enable a transaction without providing the information to the service provider," as recited in claim 1; or a method for providing a service to entities who have secure data stored in a secure registry in which each entity is identified by a multicharacter code, the service provided by a service provider, the method comprising: ... mapping the multicharacter code to information required to provide the services; providing the information to a third party without providing the information to the service provider; and using the information to enable the service provider to provide the service without the service provider's knowledge of the information, as recited in claim 16.

Thus, Applicant respectfully asserts that independent claims 1 and 16 are patentable in view of Soong at least for the above reasons. Each of claims 2, 3, 5, 8-16, 18, 19, 21 and 24-30 directly or indirectly depend from one of allowable claims 1 and 16 and are therefore patentable for at least the same reasons as the independent claim from which they depend, respectively. Claims 6, 7, 17, 22 and 23 are canceled herein. Accordingly, reconsideration and withdrawal of the rejection of claims 1-3, 5-19 and 21-30 under 35 U.S.C. §102(e) as being anticipated by Soong is respectfully requested.

Rejections Under 35 U.S.C. §103

The Office Action rejects claims 4 and 20 under 35 U.S.C. §103(a) as being unpatentable over Soong in view of U.S. Patent No. 5,398,285 to Borgelt (hereinafter Borgelt). Claim 4 depends from independent claim 1 and claim 20 depends from independent claim 16. Applicant respectfully asserts that Borgelt does not cure the deficiencies of Soong because Borgelt alone or in proper combination with Soong also does not teach or suggest "a secure registry system for providing information to a service provider to enable the service provider to provide services to

entities with secure data stored in the secure registry system, comprising ... a processor configured to receive, from the service provider, the multicharacter code for the entity on whose behalf services are to be provided, configured to map the multicharacter code to information required to provide the services where the information is unknown to the service provider, to provide the information to a third party to enable a transaction without providing the information to the service provider,” as recited in claim 1; or a “method for providing a service to entities who have secure data stored in a secure registry in which each entity is identified by a multicharacter code, the service provided by a service provider, the method comprising: receiving the multicharacter code for an entity on whose behalf the services are to be provided; mapping the multicharacter code to information required to provide the services; providing the information to a third party without providing the information to the service provider; and using the information to enable the service provider to provide the service without the service provider’s knowledge of the information,” as recited in claim 16.

Accordingly, claims 4 and 20 are patentable for at least the same reasons as claims 1 and 16, respectively. Applicant respectfully requests reconsideration and withdrawal of the rejection of claims 4 and 20 under 35 U.S.C. §103(a) as being unpatentable over Soong in view of Borgelt.

New Claims

In addition to the above, Applicant respectfully asserts that new claims 31-40 further patentably distinguish over the cited references. For example, new claim 33 recites that “the database is further configured to associate biometric information with each entity having secure data in the secure registry, respectively.” New claim 37 recites “an act of associating biometric information with each entity having secure data in the secure registry, respectively.” Applicant respectfully notes that neither Soong nor Borgelt even refer to biometric information. Accordingly, new claims 33 and 37, and claims 34-36 and 38-40 which depend therefrom, respectively, are patentable for at least this additional reason.

CONCLUSION

In view of the foregoing amendments and remarks, reconsideration is respectfully requested. This application should now be in condition for allowance; a notice to this effect is respectfully requested. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicant's attorney at the telephone number listed below.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee that is not covered by an accompanying payment, please charge any deficiency to Deposit Account No. 50/2762, Ref. No. W0537-700620.

Respectfully submitted,
Kenneth P. Weiss, Applicant

By: /Robert V. Donahoe/
Robert V. Donahoe, Reg. No. 46,667
LANDO & ANASTASI, LLP
One Main Street
Cambridge, Massachusetts 02142
United States of America
Telephone: 617-395-7000
Facsimile: 617-395-7070

Electronic Patent Application Fee Transmittal

Application Number:	11768729
Filing Date:	26-Jun-2007
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Filer:	Robert Vincent Donahoe/Fareesha Ali
Attorney Docket Number:	W0537-7006

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Claims in excess of 20	2202	5	26	130

Miscellaneous-Filing:

Petition:

Patent-Appeals-and-Interference:

Post-Allowance-and-Post-Issuance:

Extension-of-Time:

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension - 1 month with \$0 paid	2251	1	65	65
Miscellaneous:				
Total in USD (\$)				195

Electronic Acknowledgement Receipt

EFS ID:	6493372
Application Number:	11768729
International Application Number:	
Confirmation Number:	3536
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Correspondence Address:	John N. Anastasi c/o Lowrie, Lando & Anastasi, LLP Riverfront Office Park, One Main Street - Cambridge MA 02142 US 6173957000 -
Filer:	Robert Vincent Donahoe
Filer Authorized By:	
Attorney Docket Number:	W0537-7006
Receipt Date:	20-NOV-2009
Filing Date:	26-JUN-2007
Time Stamp:	14:58:46
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$195

RAM confirmation Number	1255				
Deposit Account	502762				
Authorized User					
File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		W0537-700620_Amendment.pdf	54343 cb13cacd3766ea9c49719ce9fde6a2243d2f37d9	yes	11
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Amendment/Req. Reconsideration-After Non-Final Reject		1	1	
	Claims		2	7	
	Applicant Arguments/Remarks Made in an Amendment		8	11	
Warnings:					
Information:					
2	Fee Worksheet (PTO-875)	fee-info.pdf	32136 0c06125471d79f1c95c239db7619aea389c9e9d1	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			86479		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 11/768,729	Filing Date 06/26/2007	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

APPLICATION AS FILED – PART I			OTHER THAN SMALL ENTITY				
	(Column 1)	(Column 2)	SMALL ENTITY <input checked="" type="checkbox"/>	OR			
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	OR	RATE (\$)	FEE (\$)
<input type="checkbox"/> BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>	N/A	N/A	N/A			N/A	
<input type="checkbox"/> SEARCH FEE <small>(37 CFR 1.16(k), (l), or (m))</small>	N/A	N/A	N/A			N/A	
<input type="checkbox"/> EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A	N/A			N/A	
TOTAL CLAIMS <small>(37 CFR 1.16(i))</small>	minus 20 =	*	X \$ =		OR	X \$ =	
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>	minus 3 =	*	X \$ =			X \$ =	
<input type="checkbox"/> APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.16(j))</small>							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY				
	(Column 1)	(Column 2)	(Column 3)		SMALL ENTITY	OR			
AMENDMENT	11/20/2009	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	* 34	Minus ** 30	= 4	X \$26 =	104		X \$ =	
	Independent <small>(37 CFR 1.16(h))</small>	* 2	Minus ***3	= 0	X \$110 =	0		X \$ =	
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>								
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>						OR		
					TOTAL ADD'L FEE	104	OR	TOTAL ADD'L FEE	

	(Column 1)	(Column 2)	(Column 3)						
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	*	Minus **	=	X \$ =			X \$ =	
	Independent <small>(37 CFR 1.16(h))</small>	*	Minus ***	=	X \$ =			X \$ =	
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>								
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>						OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
 ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
 *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
 The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
 //TERRANCE LAWRENCE//

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
 If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/768,729	06/26/2007	Kenneth P. Weiss	W0537-7006	3536

7590 02/03/2010
John N. Anastasi
c/o Lowrie, Lando & Anastasi, LLP
Riverfront Office Park, One Main Street
Cambridge, MA 02142

EXAMINER

DADA, BEEMNET W

ART UNIT	PAPER NUMBER
----------	--------------

2435

MAIL DATE	DELIVERY MODE
-----------	---------------

02/03/2010

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

DETAILED ACTION

This office action is in reply to an amendment filed on November 20, 2009. Claims 1, 3-5, 8, 9, 11, 16 and 21 have been amended and new claims 31-40 have been added. Claims 1-5, 8-16, 18-21, 24-40 are pending.

Response to Arguments

Applicant's arguments with respect to claims 1-5, 8-16, 18-21, 24-40 have been considered but are moot in view of the new ground(s) of rejection. Examiner would point out that the claim amendments include a phrase that is directed to negative limitation: "..where the information is unknown to the service provider..." and "...provide the service without the service provider's knowledge of the information..." *"Any negative limitation or exclusionary proviso must have basis in the original disclosure. If alternative elements are positively recited in the specification, they may be explicitly excluded in the claims. See In re Johnson, 558 F.2d 1008, 1019, 194 USPQ 187, 196 (CCPA 1977) ("[the] specification, having described the whole, necessarily described the part remaining."). See also Ex parte Grasselli, 231 USPQ 393 (Bd. App. 1983), aff 'dmem., 738 F.2d 453 (Fed. Cir. 1984). The mere absence of a positive recitation is not basis for an exclusion. Any claim containing a negative limitation which does not have basis in the original disclosure should be rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement."*

The phrase clearly recites a negative limitation. Indeed, the specification must contain a full, clear and concise description of the claimed subject matter.

Claim Rejections - 35 USC § 112

Art Unit: 2435

The following is a quotation of the first paragraph of 35 U.S.C. 112:

The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

Claims 1-5, 8-16, 18-21 and 24-40 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The specification fails to mention or teach the system/method, "...where the information is unknown to the service provider..." and "...provide the service without the service provider's knowledge of the information..."

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.


Art Unit: 2435

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BEEMNET W. DADA whose telephone number is (571)272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Beemnet W Dada/
Primary Examiner, Art Unit 2435
February 1, 2010

Search Notes 	Application/Control No. 11768729	Applicant(s)/Patent Under Reexamination WEISS, KENNETH P.
	Examiner BEEMNET W DADA	Art Unit 2435

SEARCHED			
Class	Subclass	Date	Examiner
713	169, 182, 184	2/1/10	BD
707	9	2/1/10	BD

SEARCH NOTES		
Search Notes	Date	Examiner
East search	2/1/10	BD
IEEE, Google, Citeseer	2/1/10	BD
Inventor name search	2/1/10	BD

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

--	--

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Kenneth P. Weiss
Serial No: 11/768,729
Confirmation No: 3536
Filed: June 26, 2007
For: UNIVERSAL SECURE REGISTRY

Examiner: Dada, Beemnet W.
Art Unit: 2435

CERTIFICATE OF TRANSMISSION UNDER 37 C.F.R. §1.8(a)

The undersigned hereby certifies that this document is being electronically filed in accordance with § 1.6(a)(4), on the 3rd day of May, 2010.

/Robert V. Donahoe/
Robert V. Donahoe, Reg. No. 46,667

Commissioner for Patents

AMENDMENT AFTER FINAL

Sir:

In response to the final Office Action mailed February 3, 2010, please amend the above-identified application as follows. Changes to the Claims are shown by strike through (for deleted matter) and underlining (for added matter).

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks begin on page 8 of this paper.

Amendments to the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A secure registry system for providing information to a service provider to enable the service provider to provide services to entities with secure data stored in the secure registry system, comprising:

a database including secure data for each entity, ~~wherein each entity is associated with and a~~ time-varying multicharacter code for each entity having secure data in the secure registry system, ~~respectively the multicharacter code being mapped to the secure data;~~ and

a processor configured to receive, from the service provider, the time-varying multicharacter code for the entity on whose behalf services are to be provided, configured to map the time-varying multicharacter code to secure data including information required to provide the services, the information including account identifying information where the account identifying information is unknown to the service provider, to provide the account identifying information to a third party to enable a transaction without providing the account identifying information to the service provider.

2. (Currently Amended) The system of claim 1, wherein the time-varying multicharacter code ~~represents an identity~~ is a secret code of the entity.

3. (Currently Amended) The system of claim 1, wherein the time-varying multicharacter code is provided to the system via a secure electronic transmission device.

4. (Currently Amended) The system of claim 1, wherein the time-varying multicharacter code is encrypted and transmitted to the system, and
wherein the system is configured to decrypt the time-varying multicharacter code with a public key of the entity.
5. (Currently Amended) The system as claimed in claim 1, wherein said service provider's service includes delivery, wherein the information is an address to which an item is to be delivered to the entity, wherein the system receives the time-varying multicharacter code, and
wherein the system uses the time-varying multicharacter code to obtain the appropriate address for delivery of the item by the third party.
6. (Canceled)
7. (Canceled)
8. (Canceled)
9. (Currently Amended) The secure registry system as claimed in claim ~~131~~, wherein the account identifying identity information includes credit card account information regarding the entity, and wherein the processor is configured to provide the credit card account information based upon the multicharacter code of the entity to enable the transaction.
10. (Currently Amended) The system as claimed in claim 9, wherein the system is configured to receive an approval of the credit card transaction ~~without providing the credit card number of the entity to the service provider.~~
11. (Currently Amended) The system as claimed in claim ~~131~~, wherein the account identifying identity information includes bank card account information regarding the entity, and wherein the processor is configured to provide the bank card

account information to enable the transaction based upon the multicharacter code of the entity.

12. (Currently Amended) The system as claimed in claim 11, wherein the system is configured to provide an approval of the bank card transaction ~~without providing the bank card number of the entity to the service provider.~~

13. (Currently Amended) The system as claimed in claim ~~13~~, wherein the information ~~includes~~ personal identification information regarding the entity.

14. (Currently Amended) The system as claimed in claim 13, wherein the personal identification information comprises a photograph of the entity, and wherein the photograph is provided to the service provider.

15. (Currently Amended) The system as claimed in claim 1, wherein the account identifying information ~~identifies~~ is email address information regarding the entity.

16. (Currently Amended) A method for providing a service to entities who have secure data stored in a secure registry in which each entity is identified by a time-varying multicharacter code, the service provided by a service provider, the method comprising:

receiving the time-varying multicharacter code for an entity on whose behalf the services are to be provided;

mapping the time-varying multicharacter code to information required to provide the services, the information including account identifying information unknown to the service provider;

providing the account identifying information to a third party without providing the account identifying information to the service provider; and

using the account identifying information to enable the service provider to provide the service without the service provider's knowledge of the account identifying information.

1029667.1

17. (Canceled)

18. (Currently Amended) The method of claim 16, wherein the act of receiving the time-varying multicharacter code comprises receiving a ~~secret~~ multicharacter code which represents an identity of~~is secret to~~ the entity.

19. (Currently Amended) The method of claim 16, wherein the act of receiving the time-varying multicharacter code comprises receiving the time-varying multicharacter ~~secret code which has been~~ transmitted by via a secure electronic transmission device.

20. (Currently Amended) The method of claim 16, wherein the act of receiving the time-varying multicharacter code comprises receiving an encrypted multicharacter code, and
wherein the method further comprises decrypting the encrypted multicharacter code.

21. (Currently Amended) The method as claimed in claim 16, wherein the service provider's service includes delivery, wherein the account identifying information is associated with an address to which an item is to be delivered for the entity, and wherein the third party receives the address for delivery of an item provided by the service provider.

22. (Canceled)

23. (Canceled)

24. (Currently Amended) The method as claimed in claim 16, wherein the account identifying information includes a credit card number, and wherein the act of using the account identifying information to perform the services comprises using the credit card number~~information about the entity~~ to enable a transaction.

1029667.1

25. (Currently Amended) The method as claimed in claim 24, wherein the act of using the account identifying information comprises receiving a validation or denial of the ~~credit card~~ transaction without providing the credit card number of the entity to the service provider.

26. (Currently Amended) The method as claimed in claim 16, wherein the act of using the account identifying information to perform the services comprises using bank card information about the entity to enable a transaction.

27. (Currently Amended) The method as claimed in claim 26, wherein the act of using the information comprises receiving a validation or denial of the bank card transaction without providing ~~at~~ the bank card number of the entity to the service provider.

28. (Currently Amended) The method as claimed in claim 16, wherein the act of mapping the time-varying multicharacter code to information required by the service provider comprises mapping the time-varying multicharacter code into personal identification information about the entity.

29. (Currently Amended) The method as claimed in claim 28, wherein the personal identification information comprises a photograph of the entity, and wherein the method further comprises an act of providing the photograph to the service provider.

30. (Currently Amended) The method as claimed in claim 16, wherein the account identifying information ~~identifies to~~ comprises an email address information about the entity.

31. (Canceled)

32. (Currently Amended) The method as claimed in claim 24, further comprising an act of transmitting to the service provider one of an approval or a denial of the credit card transaction ~~without providing the credit card number of the entity to the service provider.~~
33. (Previously Presented) The system of claim 1, wherein the database is further configured to associate biometric information with each entity having secure data in the secure registry, respectively.
34. (Currently Amended) The system of claim 33, wherein the processor is further configured to map the time-varying multicharacter code to biometric information associated with the entity on whose behalf the services are to be provided and to provide the biometric information to the service provider.
35. (Previously Presented) The system of claim 34, wherein the biometric information includes an image of the entity on whose behalf the services are to be provided.
36. (Currently Amended) The system of claim 34, wherein the ~~multicharacter code comprises a~~ time-varying multicharacter code is generated by a device associated with the entity on whose behalf services are to be provided.
37. (Previously Presented) The method as claimed in claim 16, further comprising an act of associating biometric information with each entity having secure data in the secure registry, respectively.
38. (Currently Amended) The method of claim 37, further comprising acts of:
mapping the time-varying multicharacter code to biometric information associated with the entity on whose behalf the services are to be provided; and
providing the biometric information to the service provider.

39. (Previously Presented) The method of claim 38, wherein the biometric information includes an image of the entity on whose behalf the services are to be provided.

40. (Canceled)

41. (New) The secure registry system of claim 1, wherein the account identifying information includes an account number.

42. (New) The secure registry system of claim 41, wherein the account identifying information includes credit card account information and the account number includes a credit card number.

43. (New) The secure registry system of claim 41, wherein the third party includes a financial service provider and the account number includes at least one of a debit card number and a credit card number.

44. (New) The secure registry of claim 43, wherein the service provider includes a merchant, and the service includes a sale of at least one of goods and services.

45. (New) The secure registry system of claim 44, wherein the processor is further configured to receive, from the service provider, a merchant ID, and a purchase amount.

REMARKS

Claims 1-5, 8-16, 18-21 and 24-40 were previously pending in this application. By this amendment, Applicant is canceling claims 8, 31 and 40 without prejudice or disclaimer. Claims 1-5, 9-16, 18-21, 24-30, 32, 34, 36 and 39 are amended herein. New claims 41-45 are added herein. As a result, claims 1-5, 9-16, 18-21, 24-30, 32-39 and 41-45 are pending for examination with claims 1 and 16 being independent claims. No new matter has been added. Support for the amendments to the claims can be found at least, for example, in the Specification as originally filed at paragraph [0078] of the published application.

Rejections Under 35 U.S.C. §112

The Office Action rejects claims 1-5, 8-16, 18-21 and 24-40 under 35 U.S.C. §112, first paragraph, as failing to comply with the written description requirement because the specification allegedly “fails to mention or teach the system/method, ‘... where the information is unknown to the service provider...’ and ‘provide the service without the service provider’s knowledge of the information.’” (Office Action at page 3.) Applicant respectfully disagrees because the specification as originally filed provides clear support such that one of ordinary skill in the art would recognize that the Applicant was in possession of all of the subject matter of claims at the time the application was filed. Because the claim amendments included herein modify some of the language which is subject to this rejection, Applicant also describes below the support for the amendments to independent claims 1 and 16 included herein.

As an initial matter, Applicant respectfully notes that compliance with the written description requirement is met when the specification conveys with reasonable clarity to those skilled in the art that, as of the filing date sought, applicant was in possession of the invention claimed. (MPEP 2163.02.) The preceding may be achieved via express, implicit, or inherent support found in the originally filed disclosure. (MPEP 2163.05.)

Applicant respectfully asserts that the application as originally filed provides clear support more than sufficient to convey with reasonable clarity to those skilled in the art that in some embodiments “information required to provide the services ... [and] unknown to the service provider ... [is provided] to a third party to enable a transaction without providing the ...

information to the service provider,” as recited in claim 1. As one example, at paragraph [0018] the specification describes that:

In a financial context, providing anonymous identification of a person enables the person to purchase goods and/or services from a merchant without ever transmitting to the merchant information, such as the person's credit card number, or even the person's name, that could be intercepted and/or usurped and used in subsequent or additional unauthorized transactions or for other undesired purposes. (Emphasis added.)

Further, describing and embodiment illustrated in Fig. 7, at paragraph [0078] the specification describes that in one embodiment, “the user has been able to purchase goods or services from a merchant without ever providing to the merchant the credit card number” and then at paragraph [0079], “[a]nother embodiment of a system for facilitating purchase of goods or services without providing financial information to the merchant is set forth in FIG. 8.” (Emphasis added.) At paragraph [0080], the specification describes that “[i]n this embodiment, like the embodiment of FIG. 7, the user can use the USR system 10 to purchase goods or services from a merchant without providing the merchant with the user's credit card number.” (Emphasis added.) Still further, at paragraph [0086] the specification describes an embodiment illustrated in Fig. 9 in which a “check verification system may take place over an unsecured connection between the merchant and the USR system 10 since the user's bank account information is not sent over the connection between the merchant and the USR system 10.” (Emphasis added.) The specification describes still another embodiment in paragraph [0088] stating that Fig. 10 “illustrates a method of conducting a transaction with a merchant without requiring the user to provide to the merchant the user's name, address, or other identifying information, while enabling the merchant to ship the goods to the user.” (Emphasis added.)

Applicant respectfully asserts that each of the preceding examples provide express, implicit and inherent support more than sufficient to convey to one of ordinary skill in the art that “information required to provide the services ... [and] unknown to the service provider ... [is provided] to a third party to enable a transaction without providing the ... information to the service provider,” as recited in claim 1. In addition, Applicant respectfully asserts that each of the preceding examples provide express, implicit and inherent support more than sufficient to convey to one of ordinary skill in the art a “method for providing a service to entities who have

secure data stored in a secure registry in which each entity is identified by a time-varying multicharacter code, the service provided by a service provider, the method comprising ... mapping the time-varying multicharacter code to information required to provide the services, the information including account identifying information unknown to the service provider; providing the account identifying information to a third party without providing the account identifying information to the service provider; and using the account identifying information to enable the service provider to provide the service without the service provider's knowledge of the account identifying information," as recited in claim 16.

In addition, Applicant has amended each of claims 1 and 16 to recite that the "information unknown to the service provider" includes "account identifying information unknown to the service provider." (Emphasis added.) This amendment is also clearly supported in the specification, for example, in some of the examples described above.

At page 2, the Office Action describes the language recited in claim 1 as being directed to "a negative limitation," and alleges that the language does not have a basis in the original disclosure. Applicant respectfully disagrees and asserts that the above provides citations where express support can be found for the language of claims 1 and 16.

For at least all of the above reasons, Applicant respectfully requests reconsideration and withdrawal of the rejection of claims 1-5, 8-16, 18-21 and 24-40 under 35 U.S.C. §112, first paragraph.

CONCLUSION

In view of the foregoing amendments and remarks, reconsideration is respectfully requested. This application should now be in condition for allowance; a notice to this effect is respectfully requested. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicant's attorney at the telephone number listed below.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee that is not covered by an accompanying payment, please charge any deficiency to Deposit Account No. 50/2762, Ref. No. W0537-700620.

Respectfully submitted,
Kenneth P. Weiss, Applicant

By: /Robert V. Donahoe/
Robert V. Donahoe, Reg. No. 46,667
LANDO & ANASTASI, LLP
One Main Street
Cambridge, Massachusetts 02142
United States of America
Telephone: 617-395-7000
Facsimile: 617-395-7070

Docket No.: W0537-700620

Date: May 3, 2010

Electronic Patent Application Fee Transmittal

Application Number:	11768729
Filing Date:	26-Jun-2007
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Filer:	Robert Vincent Donahoe/Fareesha Ali
Attorney Docket Number:	W0537-7006

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Claims in excess of 20	2202	2	26	52

Miscellaneous-Filing:

Petition:

Patent-Appeals-and-Interference:

Post-Allowance-and-Post-Issuance:

Extension-of-Time:

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				52

Electronic Acknowledgement Receipt

EFS ID:	7537371
Application Number:	11768729
International Application Number:	
Confirmation Number:	3536
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Correspondence Address:	John N. Anastasi c/o Lowrie, Lando & Anastasi, LLP Riverfront Office Park, One Main Street - Cambridge MA 02142 US 6173957000 -
Filer:	Robert Vincent Donahoe
Filer Authorized By:	
Attorney Docket Number:	W0537-7006
Receipt Date:	03-MAY-2010
Filing Date:	26-JUN-2007
Time Stamp:	16:57:36
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$52

RAM confirmation Number	3800				
Deposit Account	502762				
Authorized User					
File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		W0537-700620_Amendment_After_Final.pdf	59485 <small>e2920c059980cbf43582c7a4392096de39e484b</small>	yes	12
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Amendment After Final		1	1	
	Claims		2	8	
	Applicant Arguments/Remarks Made in an Amendment		9	12	
Warnings:					
Information:					
2	Fee Worksheet (PTO-875)	fee-info.pdf	30090 <small>d95c0a5fc79a330b1ba72bae4f4681592f55e0be</small>	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			89575		
<p>This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.</p> <p><u>New Applications Under 35 U.S.C. 111</u> If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.</p> <p><u>National Stage of an International Application under 35 U.S.C. 371</u> If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.</p> <p><u>New International Application Filed with the USPTO as a Receiving Office</u> If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.</p>					

Document code: WFEE

United States Patent and Trademark Office
Sales Receipt for Accounting Date: 05/05/2010

YSHORT	SALE	#00000004	Mailroom Dt:	05/03/2010	502762	11768729
		01	FC : 2202	26.00	DA	

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 11/768,729	Filing Date 06/26/2007	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

APPLICATION AS FILED – PART I			OTHER THAN SMALL ENTITY				
	(Column 1)	(Column 2)	SMALL ENTITY <input checked="" type="checkbox"/>	OR			
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	OR	RATE (\$)	FEE (\$)
<input type="checkbox"/> BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>	N/A	N/A	N/A			N/A	
<input type="checkbox"/> SEARCH FEE <small>(37 CFR 1.16(k), (l), or (m))</small>	N/A	N/A	N/A			N/A	
<input type="checkbox"/> EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A	N/A			N/A	
TOTAL CLAIMS <small>(37 CFR 1.16(i))</small>	minus 20 =	*	X \$ =		OR	X \$ =	
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>	minus 3 =	*	X \$ =			X \$ =	
<input type="checkbox"/> APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.16(j))</small>							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY				
	(Column 1)	(Column 2)	(Column 3)		SMALL ENTITY	OR			
AMENDMENT	05/03/2010	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	* 37	Minus ** 34	= 3	X \$26 =	78	OR	X \$ =	
	Independent <small>(37 CFR 1.16(h))</small>	* 2	Minus ***3	= 0	X \$110 =	0	OR	X \$ =	
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>								
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>						OR		
					TOTAL ADD'L FEE	78	OR	TOTAL ADD'L FEE	

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY				
	(Column 1)	(Column 2)	(Column 3)		SMALL ENTITY	OR			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	*	Minus **	=	X \$ =		OR	X \$ =	
	Independent <small>(37 CFR 1.16(h))</small>	*	Minus ***	=	X \$ =		OR	X \$ =	
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>								
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>						OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
 ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
 *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
 The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/VIKKI SHORT/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**
 If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/768,729	06/26/2007	Kenneth P. Weiss	W0537-7006	3536

7590 05/13/2010
John N. Anastasi
c/o Lowrie, Lando & Anastasi, LLP
Riverfront Office Park, One Main Street
Cambridge, MA 02142

EXAMINER

DADA, BEEMNET W

ART UNIT	PAPER NUMBER
----------	--------------

2435

MAIL DATE	DELIVERY MODE
-----------	---------------

05/13/2010

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

**Advisory Action
Before the Filing of an Appeal Brief**

Application No. 11/768,729	Applicant(s) WEISS, KENNETH P.	
Examiner BEEBNET W. DADA	Art Unit 2435	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 03 May 2010 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:

- a) The period for reply expires 3 months from the mailing date of the final rejection.
- b) The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.
- Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
- (a) They raise new issues that would require further consideration and/or search (see NOTE below);
- (b) They raise the issue of new matter (see NOTE below);
- (c) They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
- (d) They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: See Continuation Sheet. (See 37 CFR 1.116 and 41.33(a)).

4. The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. Applicant's reply has overcome the following rejection(s): _____.
6. Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. For purposes of appeal, the proposed amendment(s): a) will not be entered, or b) will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
- The status of the claim(s) is (or will be) as follows:
- Claim(s) allowed: _____.
- Claim(s) objected to: _____.
- Claim(s) rejected: 1-5, 8-16, 18-21 and 24-40.
- Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. The request for reconsideration has been considered but does NOT place the application in condition for allowance because: _____.
12. Note the attached Information *Disclosure Statement*(s). (PTO/SB/08) Paper No(s). _____
13. Other: _____.

/Beemnet W Dada/
Primary Examiner, Art Unit 2435

Continuation of 3. NOTE: new claim language would require further consideration.

Docket No.: W0537-700620

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Kenneth P. Weiss
Serial No: 11/768,729
Confirmation No: 3536
Filed: June 26, 2007
For: UNIVERSAL SECURE REGISTRY

Examiner: Dada, Beemnet W.
Art Unit: 2435

CERTIFICATE OF TRANSMISSION UNDER 37 C.F.R. §1.8(a)

The undersigned hereby certifies that this document is being electronically filed in accordance with § 1.6(a)(4), on the 3rd day of May, 2010.

/Robert V. Donahoe/
Robert V. Donahoe, Reg. No. 46,667

Commissioner for Patents

DO NOT ENTER: /BD/

AMENDMENT AFTER FINAL

Sir:

In response to the final Office Action mailed February 3, 2010, please amend the above-identified application as follows. Changes to the Claims are shown by strike through (for deleted matter) and underlining (for added matter).

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks begin on page 8 of this paper.

**REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL
(Submitted Only via EFS-Web)**

Application Number	11768729	Filing Date	2007-06-26	Docket Number (if applicable)	W0537-700620	Art Unit	2435
First Named Inventor	Kenneth P. Weiss			Examiner Name	Dada, Beemnet W.		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

Other _____

Enclosed

Amendment/Reply

Information Disclosure Statement (IDS)

Affidavit(s)/ Declaration(s)

Other _____

MISCELLANEOUS

Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

Other 1 Month Extension of Time

FEES

The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.

The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 502762

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Patent Practitioner Signature

Applicant Signature

Signature of Registered U.S. Patent Practitioner			
Signature	/Robert V. Donahoe/	Date (YYYY-MM-DD)	2010-05-24
Name	Robert V. Donahoe	Registration Number	46667

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11768729
	Filing Date	2007-06-26
	First Named Inventor	Kenneth P. Weiss
	Art Unit	2435
	Examiner Name	Dada, Beemnet W.
	Attorney Docket Number	W0537-700620

U.S.PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1						

If you wish to add additional U.S. Patent citation information please click the Add button. Add

U.S.PATENT APPLICATION PUBLICATIONS							Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1	20010044900		2001-11-22	Uchida		
	2	20030115490		2003-06-19	Russo et al.		
	3	20050187843		2005-08-25	Lapsley et al.		
	4	20050001711		2005-01-06	Doughty		
	5	20060016884		2006-01-26	Block et al.		

If you wish to add additional U.S. Published Application citation information please click the Add button. Add

FOREIGN PATENT DOCUMENTS							Remove
--------------------------	--	--	--	--	--	--	--------

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	11768729
Filing Date	2007-06-26
First Named Inventor	Kenneth P. Weiss
Art Unit	2435
Examiner Name	Dada, Beemnet W.
Attorney Docket Number	W0537-700620

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² i	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	1996036934	WO		1996-11-21	Smart Touch, L.L.C.		<input type="checkbox"/>
	2	0 986 209	EP		2000-03-15	Mitsubishi Denki Kabushiki Kaisha		<input type="checkbox"/>
	3	2002014985	WO		2002-02-21	Kern		<input type="checkbox"/>

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1		<input type="checkbox"/>

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	Date Considered
--------------------	-----------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11768729
	Filing Date	2007-06-26
	First Named Inventor	Kenneth P. Weiss
	Art Unit	2435
	Examiner Name	Dada, Beemnet W.
	Attorney Docket Number	W0537-700620

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

Fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

None

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Robert V. Donahoe/	Date (YYYY-MM-DD)	2010-05-24
Name/Print	Robert V. Donahoe	Registration Number	46667

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

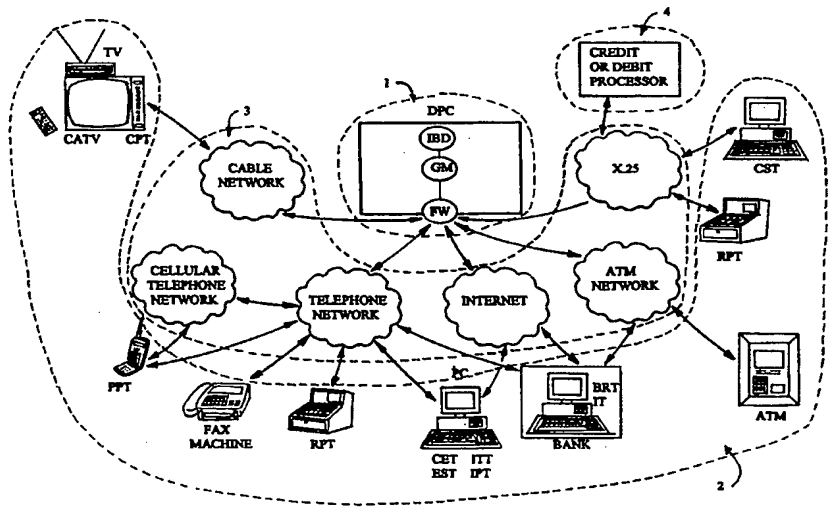
1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification ⁶ : G06K 9/00</p>	<p>A1</p>	<p>(11) International Publication Number: WO 96/36934 (43) International Publication Date: 21 November 1996 (21.11.96)</p>
<p>(21) International Application Number: PCT/US96/07185 (22) International Filing Date: 17 May 1996 (17.05.96) (30) Priority Data: 08/442,895 17 May 1995 (17.05.95) US (71) Applicant: SMART TOUCH, L.L.C. [US/US]; Suite 12, 46 Shattuck Square, Berkeley, CA 94704 (US). (72) Inventors: HOFFMAN, Ned; Suite 12, 46 Shattuck Square, Berkeley, CA 94704 (US). PARE, David, F.; Suite 12, 46 Shattuck Square, Berkeley, CA 94704 (US). LEE, Jonathan, A.; Suite 12, 46 Shattuck Square, Berkeley, CA 94704 (US). (74) Agent: KAMAREI, Ali; Suite 12, 46 Shattuck Square, Berkeley, CA 94704 (US).</p>		<p>(81) Designated States: AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, ES, FI, GB, GE, HU, JP, KE, KG, KP, KR, KZ, LK, LT, LU, LV, MD, MG, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SI, SK, TJ, TT, UA, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).</p> <p>Published <i>With international search report.</i></p>

(54) Title: TOKENLESS IDENTIFICATION SYSTEM FOR AUTHORIZATION OF ELECTRONIC TRANSACTIONS AND ELECTRONIC TRANSMISSIONS



(57) Abstract

A tokenless identification system and method are principally based on a correlative comparison of a unique biometrics sample, such as a finger print or voice recording, gathered directly from the person of an unknown user, with an authenticated biometrics sample of the same type obtained and stored previously (1). It can be networked to act as a full or partial intermediary between other independent computer systems (3), or maybe the sole computer systems carrying out all necessary executions.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	GB	United Kingdom	MW	Malawi
AT	Austria	GE	Georgia	MX	Mexico
AU	Australia	GN	Guinea	NE	Niger
BB	Barbados	GR	Greece	NL	Netherlands
BE	Belgium	HU	Hungary	NO	Norway
BF	Burkina Faso	IE	Ireland	NZ	New Zealand
BG	Bulgaria	IT	Italy	PL	Poland
BJ	Benin	JP	Japan	PT	Portugal
BR	Brazil	KE	Kenya	RO	Romania
BY	Belarus	KG	Kyrgystan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic	KR	Republic of Korea	SE	Sweden
CG	Congo	KZ	Kazakhstan	SG	Singapore
CH	Switzerland	LI	Liechtenstein	SI	Slovenia
CI	Côte d'Ivoire	LK	Sri Lanka	SK	Slovakia
CM	Cameroon	LR	Liberia	SN	Senegal
CN	China	LT	Lithuania	SZ	Swaziland
CS	Czechoslovakia	LU	Luxembourg	TD	Chad
CZ	Czech Republic	LV	Larvia	TG	Togo
DE	Germany	MC	Monaco	TJ	Tajikistan
DK	Denmark	MD	Republic of Moldova	TT	Trinidad and Tobago
EE	Estonia	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	UG	Uganda
FI	Finland	MN	Mongolia	US	United States of America
FR	France	MR	Mauritania	UZ	Uzbekistan
GA	Gabon			VN	Viet Nam

**TOKENLESS IDENTIFICATION SYSTEM FOR
AUTHORIZATION OF ELECTRONIC TRANSACTIONS AND
ELECTRONIC TRANSMISSIONS**

By:
Ned Hoffman
David Pare
Jonathan Lee

Cross-Reference

The present application is a continuation-in-part of United States Patent Application Serial No. 08/345,523, filed November 28, 1994, which is incorporated herein by reference.

Background

The use of tokens and credit cards in today's financial world is pervasive. A token would be any inanimate object which confers a capability to the individual presenting the object. Remote access of every financial account is through the use of tokens or plastic cards. Whether buying groceries with debit cards or consumer goods with credit cards, at the heart of that transaction is a money transfer enabled by a token, which acts to identify an individual and the financial account he is accessing.

The reason for the migration from metal coins to plastic cards is simple and straightforward: access to money in this money transfer system is vastly safer and more convenient for both merchants and consumers than handling large quantities of coins and notes.

Unfortunately, current technology in combination with this convenient token-based money transfer system results in a system that is prone to theft and fraud.

As verification of user identity is based solely on data placed on the token, which can be easily reproduced and transferred between individuals, such security must rely on both the diligence and the luck of the authorized user and merchant in maintaining this information as proprietary. However, by their very nature, tokens do not have a very strong connection with the individual. Identification of the rightful owner of the token through the token is tenuous at best. This is easily

demonstrated by the fact that individuals other than the rightful owners of the tokens have been using these tokens to defraud merchants and other consumer goods suppliers.

5 The mammoth expansion of the consumer credit industry during the 1980s brought with it large profits for issuers, and newfound convenience for consumers. However, as consumer credit became easier for consumers to acquire, it also became a target for criminals. Much as the mobility of the automobile led to a rash of bank robberies in the late 1920's and early 1930's, so too did the ubiquity of consumer credit lead to vastly increased opportunities for criminals.

10 Initially, the banking industry was willing to accept a certain amount of loss due to fraud, passing the cost on to the consumer. However, as criminals became more organized, more technically adept, and as credit retail stations began to be manned by people who were more and more poorly trained in credit card security matters, the rate of increase of fraud losses skyrocketed. The staggering statistics on fraud and cost of preventive steps, has forced the credit card companies in particular, to look for other solutions to the problem.

15 Fraud losses in the credit card industry stem from many different areas due to the highly vulnerable nature of the system, but they are mainly due to either lost, stolen, or counterfeit cards. Credit cards operate without the use of a personal identification code (PIC), therefore a lost credit card can be turned into cash if the card falls into the wrong hands. While theft of a token constitutes the majority of fraud in the system, the use of counterfeit credit cards has been on the rise. Counterfeit credit cards are manufactured by a more technically sophisticated criminal by acquiring a cardholder's valid account number and then producing a counterfeit card using that valid number. The counterfeiter encodes the magnetic strip, and embosses the counterfeit plastic card with the account number. The card is then presented to merchants and charged up to the rightful cardholder's account. Another form of loss is by a criminal merchant who surreptitiously obtains the cardholder's account number. Yet another type of fraud is committed by the authorized cardholder when the token is used for making purchases and thereafter a claim is made that the token was either lost or stolen. It is estimated that losses due to all types of fraud exceeds \$950 million dollars annually.

20
25
30
35

Generally, debit cards are used in conjunction with a personal identification code (PIC). Counterfeiting a debit card is more difficult as the criminal must acquire not only the account number, but also the PIC, and then manufacture the card as in the credit card example. However, various strategies have been used to obtain PICs from unwary cardholders; these range from Trojan horse automated teller machines, or ATMs, in shopping malls that dispense cash but record the PIC, to merchant point of sale devices that also record the PIC, to individuals with binoculars that watch cardholders enter PICs at ATMs. The subsequently manufactured counterfeit debit cards are then used in various ATM machines until the unlucky account is emptied.

The financial industry is well aware of the trends in fraud expense, and is constantly taking steps to improve the security of the card. Thus fraud and theft of token have an indirect impact on the cost to the system.

Card blanks are manufactured under very tight security. Then they are individualized with the account number, expiration date, and are then mailed to the cardholder. Manufacturing and distributing the card alone costs the industry approximately one billion dollars annually. The standard card costs the financial industry \$2 for each, but only \$0.30 of this \$2 is associated with actual manufacturing cost.

Over the last ten years, the industry has altered the tokens because of counterfeiting fraud, without any fundamental changes in the use of the credit transaction system. The remedy has been mostly administrative changes such as having customers call the issuer to activate their card. Other changes include addition of a hologram, a picture ID, or an improved signature area. These type of changes in particular, are an indication that the systems susceptibility to fraud is due to lack of true identification of the individual. It is estimated that this could double the manufacturing cost to two billion dollars annually.

In the near future, the banking industry expects to move to an even more expensive card, called a "smart card". Smart cards contain as much computing power as did some of the first home computers. Current cost projections for a first-generation smart card is estimated at approximately \$3.50, not including distribution costs, which is significantly higher than the \$0.30 plastic card blank.

5 This significant increase in cost has forced the industry to look for new ways of using the power in the smart card in addition to simple transaction authorization. It is envisioned that in addition to storing credit and debit account numbers, smart cards may also store phone numbers, frequent flyer miles, coupons obtained from stores, a transaction history, electronic cash usable at tollbooths and on public transit systems, as well as the customer's name, vital statistics, and perhaps even medical records. Clearly, the financial industry trend is to further establish use of tokens.

10 The side effect of increasing the capabilities of the smart card is centralization of functions. The flip side of increased functionality is increased vulnerability. Given the number of functions that the smart card will be performing, the loss or damage of this monster card will be excruciatingly inconvenient for the cardholder. Being without such a card will financially incapacitate the cardholder until it is replaced. Additionally, losing a card full of electronic cash will also result in a real financial loss as well. Furthermore, ability of counterfeiters to one day copy a smartcard is not addressed.

15 Unfortunately, because of the projected concentration of functions onto the smart card, the cardholder is left more vulnerable to the loss or destruction of the card itself. Thus, after spending vast sums of money, the resulting system will be more secure, but threatens to levy heavier and heavier penalties for destruction or loss of this card on the consumer.

20 The financial industry recognizes the security issues associated with smartcards, and efforts are currently underway to make each plastic card difficult to counterfeit. Billions of dollars will be spent in the next five years in attempts to make plastic ever more secure. To date, the consumer financial transaction industry has had a simple equation to balance: in order to reduce fraud, the cost of the card must increase.

25 In addition to and associated with the pervasiveness of electronic financial transactions, there is now the widespread use of electronic facsimiles, electronic mail messages and similar electronic communications. Similar to the problem of lack of proper identification of individuals for financial transactions is the problem of lack of proper identification of individuals for electronic transmissions. The ease and

30

35

speed of electronic communication, and its low cost compared to conventional mail, has made it a method of choice for communication between individuals and businesses alike. This type of communication has expanded greatly and is expected to continue to expand. However, millions of electronic messages such as facsimiles and electronic mail (or "E-mail" or "email") messages are sent without knowing whether they arrive at their true destination or whether a certain individual actually sent or received that electronic message. Furthermore, there is no way to verify the identify the individual who sent or who received an electronic message.

Recently, various attempts have been made to overcome problems inherent in the token and code security system. One major focus has been to encrypt, variablize or otherwise modify the PIC to make it more difficult for an unauthorized user to carry out more than one transaction, largely by focusing on manipulation of the PIC to make such code more fraud resistant. A variety of approaches have been suggested, such as introducing an algorithm that varies the PIC in a predictable way known only to the user, thereby requiring a different PIC code for each subsequent accessing of an account. For example, the PIC code can be varied and made specific to the calendar day or date of the access attempt. In yet another approach, a time-variable element is introduced to generate a non-predictable personal identification code that is revealed only to an authorized user at the time of access. Although more resistant to fraud than systems incorporating non-variable codes, such an approach is not virtually fraud-proof because it still relies on data that is not uniquely and irreproducibly personal to the authorized user. Furthermore, such systems further inconvenience consumers that already have trouble remembering constant codes, much less variable ones. Examples of these approaches are disclosed in United States Patents 4,837,422 to Dethloff et al.; 4,998,279 to Weiss; 5,168,520 to Weiss; 5,251,259 to Mosley; 5,239,538 to Parrillo; 5,276,314 to Martino et al.; and 5,343,529 to Goldfine et al. all of which are incorporated herein by reference.

More recently, some have turned their attention from the use of personal identification codes to the use of unique biometrics as the basis of identity verification, and ultimately computer access. In this approach, authenticated biometrics are recorded from a user of known identity and stored for future reference on a token. In every subsequent access attempt,

5 the user is required to enter physically the requested biometrics, which are
then compared to the authenticated biometrics on the token to determine if
the two match in order to verify user identity. Because the biometrics are
uniquely personal to the user and because the act of physically entering the
biometrics are virtually irreproducible, a match is putative of actual
identity, thereby decreasing the risk of fraud. Various biometrics have been
suggested, such as finger prints, hand prints, voice prints, retinal images,
handwriting samples and the like. However, because the biometrics are
10 generally stored in electronic (and thus reproducible) form on a token and
because the comparison and verification process is not isolated from the
hardware and software directly used by the individual attempting access, a
significant risk of fraudulent access still exists. Examples of this approach
to system security are described in United States Patents 4,821,118 to
Lafreniere; 4,993,068 to Piosenka et al.; 4,995,086 to Lilley et al.;
15 5,054,089 to Uchida et al.; 5,095,194 to Barbanell; 5,109,427 to Yang;
5,109,428 to Igaki et al.; 5,144,680 to Kobayashi et al.; 5,146,102 to
Higuchi et al.; 5,180,901 to Hiramatsu; 5,210,588 to Lee; 5,210,797 to
Usui et al.; 5,222,152 to Fishbine et al.; 5,230,025 to Fishbine et al.;
20 5,241,606 to Horie; 5,265,162 to Bush et al.; 5,321,242 to Heath, Jr.;
5,325,442 to Knapp; 5,351,303 to Willmore, all of which are incorporated
herein by reference.

As will be appreciated from the foregoing discussion, a dynamic
but unavoidable tension arises in attempting to design a security system
that is highly fraud resistant, but nevertheless easy and convenient for the
25 consumer to use. Unfortunately, none of the above-disclosed proposed
improvements to the token and code system adequately address, much less
attempt to balance, this tension. Such systems generally store the
authenticated biometrics in electronic form directly on the token that can
presumably be copied. Further, such systems do not adequately isolate the
30 identity verification process from tampering by someone attempting to gain
unauthorized access.

35 An example of token-based security system which relies on a
biometrics of a user can be found in United States Patent 5,280,527 to
Gullman et al. In Gullman's system, the user must carry and present a
credit card sized token (referred to as a biometrics security apparatus)
containing a microchip in which is recorded characteristics of the

5 authorized user's voice. In order to initiate the access procedure, the user must insert the token into a terminal such as an ATM, and then speak into the terminal to provide a biometrics input for comparison with an authenticated input stored in the microchip of the presented token. The process of identity verification is generally not isolated from potential tampering by one attempting unauthorized access. If a match is found, the remote terminal may then signal the host computer that access should be permitted, or may prompt the user for an additional code, such as a PIN (also stored on the token), before sending the necessary verification signal to the host computer.

10 Although Gullman's reliance of comparison of stored and input biometrics potentially reduces the risk of unauthorized access as compared to numeric codes, Gullman's use of the token as the repository for the authenticating data combined with Gullman's failure to isolate the identity verification process from the possibility of tampering greatly diminishes any improvement to fraud resistance resulting from the replacement of a numeric code with a biometrics. Further, the system remains somewhat cumbersome and inconvenient to use because it too requires the presentation of a token in order to initiate an access request.

15 Almost uniformly, patents that disclose token-based systems teach away from biometrics recognition without the use of tokens. Reasons cited for such teachings range from storage requirements for biometrics recognition systems to significant time lapses in identification of a large number of individuals, even for the most powerful computers.

20 In view of the foregoing, there has long been a need for a computer access system that is highly fraud-resistant, practical, and efficient for the user to operate and carry out electronic transactions and transmissions expeditiously.

25 There is also a need for a computer system that is completely tokenless and that is capable of verifying a user's personal identity, based solely upon a personal identification code and biometrics that is unique and physically personal to an authorized user, as opposed to verifying an individual's possession of any physical objects that can be freely transferred between different individuals. Such biometrics must be easily and non-intrusively obtained; must be easy and cost-effective to store and to analyze; and must not unduly invade the user's privacy rights.

5 A further need in computer access system design is user convenience. It is highly desirable for a consumer to be able to access the system spontaneously, particularly when unexpected needs arise, with a minimum of effort. In particular, there is a need for a system that greatly reduces or eliminates the need to memorize numerous or cumbersome codes, and that eliminates the need to possess, carry, and present a proprietary object in order to initiate an access request.

10 Such systems must be simple to operate, accurate and reliable. There is also a need for a computer access system that can allow a user to access multiple accounts and procure all services authorized to the user, and carry out transactions in and between all financial accounts, make point of purchase payments, receive various services, etc.

15 There is further a great need for a computer access system that affords an authorized user the ability to alert authorities that a third party is coercing the user to request access without the third party being aware that an alert has been generated. There is also a need for a system that is nevertheless able to effect, unknown to the coercing third party, temporary restrictions on the types and amounts of transactions that can be undertaken once access is granted.

20 Furthermore, the computer system must be affordable and flexible enough to be operatively compatible with existing networks having a variety of electronic transaction and transmission devices and system configurations.

25 Finally, there is a need for secured sending and receipt of electronic mail messages and electronic facsimiles, where content of the electronic message is protected from disclosure to unauthorized individuals, and the identity of the sender or recipient can be obtained with a high degree of certainty.

30 Summary of the Invention

35 The present invention satisfies these needs by providing an improved identification system for determining an individual's identity from a comparison of an individual's biometrics sample and personal identification code gathered during a bid step with biometrics sample and personal identification code for that individual gathered during a registration step and stored at a remote site wherein there is a data

5 processing center. The invention comprises a computer network host system with means for comparing the entered biometrics sample and personal identification code, and is equipped with various data bases and memory modules. Furthermore, the invention is provided with biometrics and personal identification code input apparatus and terminals for entering data to provide information for execution of the requested transactions and transmissions by the host system once the identity of the individual is determined. The invention is also provided with means for connecting the host system with the terminal and the biometrics input apparatus.

10 The computer also has means for execution of various transactions and transmission in addition to traditional storing of and modification of data. Additionally, the computer can output the evaluation of the biometrics- PIC ("personal identification code") comparison, and the determination of an identification evaluation, or status of any execution of transactions or transmissions. Furthermore, the computer system notifies and authenticates to the individual being identified that the computer system was accessed, by returning to the individual a private code which was previously selected by that individual during the registration step.

15 Preferably, the computer system is protected from electronic eavesdropping and electronic intrusion and viruses. Further, the devices used by the computer for gathering biometric samples and personal identification codes would comprise: a) at least one biometric input device for gathering biometric samples, which would have a hardware and a software component; b) at least one terminal device that is functionally partially or fully integrated with the biometric input means for input of and appending ancillary information; c) at least one data entry device for input of a personal identification code whereby this data entry device is integrated either with the biometric input device or the terminal device; and, d) a means for interconnecting the biometric input device, data entry device and the terminal. The terminal device also has at least one display device for displaying data and information. For additional security the computer system uniquely identifies the biometric input apparatus, and the counter party or merchant through a counter party or merchant identification code relating to the terminal that is connected to the biometric input device. It is also preferred that the biometric input apparatus be secured from physical and electronic tampering, and that in

20
25
30
35

case of physical breach of the device, means be employed to physically and/or electronically destroy components within the apparatus and/or erase critical data from the device's memory modules.

5 In addition, the biometric input apparatus would have a hardware component comprising: a) at least one computing module for data processing; b) erasable and non-erasable memory modules for storage of data and software; c) a biometric scanner device for input of biometric data; d) a data entry device for entering data; e) a digital communications port; f) a device for prevention of electronic eavesdropping.

10 In order to protect the integrity and confidentiality of electronic data sent between the biometric input apparatus, the terminal, and the computer network, it is preferred that the data be encrypted and sealed.

15 The host computer network is also connected to and is able to communicate with other independent computer systems, databases, facsimile machines, and other computer networks through conventional means.

20 The method of the present invention includes voluntarily identifying an individual without the use of any tokens by means of examination of at least one biometrics sample provided by that the individual and a personal identification code also provided by that individual. During a registration step, the individual is to register with the system an authenticated biometric sample, a personal identification code and a private code. Thereafter, during a bid step the biometrics sample and personal identification code of the individual is gathered and compared to the ones registered during the registration step. A match of the personal identification codes and biometrics sample will result in the positive
25 identification of the individual. In order to authenticate to the identified individual that the real computer system was accessed, the individual's private code, which was collected at the registration step, is returned to the individual.

30 It is preferred that the method of the invention include a method for examining the biometrics samples during registration and comparing such biometrics with a collection of biometrics samples from individuals who have been designated as having previously attempted to perpetrate or
35 who have actually perpetrated fraud upon the system.

In a preferred embodiment, the invention includes a method for notifying authorities of the presence of exigent circumstances or that the authorized user is under duress.

5 It is also preferred that a method of encryption and sealing of data be used to protect the data, including the digitized biometrics sample, from being revealed accidentally or unveiled from criminal elements during transmission.

10 It is also preferred that the method include steps for the individual to choose various financial accounts, and choose various modes of electronic transmissions.

It is also preferred that the method include a method for archiving of data and electronic transmissions, and retrieval of the archived data using a tracking code.

15 It is furthermore preferred that any document, such as a facsimile or an electronic mail message be uniquely checksummed using algorithm for future identification of the document.

20 Yet another method of the invention is to be able to rapidly identify an individual from an examination of his biometrics sample and personal identification code by storing several dissimilar biometrics samples from different individuals in an electronic basket that is identified by one personal identification code.

25 In one embodiment of the invention, the computer system can allow individuals to select their own personal identification code (or "PIC") from a group of PICs selected by the remote data processing center. This is performed in a method whereby once the individual's biometric is gathered, the data processing center selects several PICs at random which may be conducive to being memorized. The data processing center then conducts a comparison of the biometric gathered with those already in those PIC baskets or groups. In the event the new registrant's biometric is too similar
30 to any previously registered biometric which has been allotted to any one of those randomly selected PIC groups, then that PIC is rejected by the database for use by the new individual and an alternative PIC is selected for another such biometric comparison. Once the data processing center has generated several PIC options without a confusingly similar biometric,
35 those PICs are presented to the new registrant from which the individual may select one PIC .

In one embodiment of the invention, there is a method for rapid search of at least one first previously stored biometric sample from a first individual, using a personal identification code-basket that is capable of containing at least one algorithmically unique second biometric sample that is from at least one second individual, and which is identified by said personal identification code-basket, comprising, firstly, a storage step further comprising: a) the selection of a private code by a first individual; b) the selection of a personal identification code by said first individual; c) the entering a biometric sample from said first individual; d) locating the personal identification code-basket identified by the personal identification code selected by said first individual; e) comparison of the biometric sample taken from said first individual with any previously stored biometric samples in said selected personal identification code-basket to make sure that the biometric sample entered by said first individual is algorithmically unique from the previously stored at least one biometric sample provided by at least one second individual, and; f) storage of the entered biometric sample from said first individual in the selected personal identification code-basket if said sample is algorithmically unique from the at least one previously stored biometric sample from said at least one second individual. There is also a bid step further comprising: a) entering said selected personal identification code by said first individual, and; b) entering a biometric sample by said first individual. There is also a comparison step comprising: a) finding the personal identification code-basket that is identified by said personal identification code entered by said first individual, and; b) comparison of the entered biometric sample from said first individual with said at least one stored biometric sample from said at least one second individual in said entered personal identification code-basket for producing either a successful or failed identification result. There could also be: a) an execution step wherein a command is processed and executed to produce a determination; b) an output step wherein said identification result or said determination is externalized and displayed, and; c) a presentation step wherein on successful identification of said first individual, said private code is presented to said first individual.

According to one embodiment of the invention, the host system is positioned in series between the individual being identified and other computer networks that are to be accessed, thereby acting as an interface. It will be appreciated that in this embodiment, the user tenders an access request directly to the host computer system of the invention, which is operationally interactive with other independent secured computer systems such as VISANET. The computer system would therefore maintain authenticated biometrics data samples for all authorized users of each secured computer system that it services. These data would be cross-referenced by each authorized user. Thus, after identity verification is completed, the security system provides to the user a listing of systems that he is authorized to access, and prompts the user to select the desired network. Thereafter, the requested execution step and information regarding the transaction is forwarded to the selected independent computer network similar to the type of communications sent today between merchants and credit card companies.

In a second embodiment the host system may also carry out the functions of the other independent computer systems such as debiting or crediting a financial account. In this system, the computer system of the invention carries out the functions requested by the individual without use of external, independent computer networks.

According to a further embodiment of the invention, a means is provided for alerting predesignated authorities during an access attempt during which the user has been coerced by a third party to request access to the host computer system. In such an embodiment, an authorized user would have a number of codes, most of which would be recognized by the computer system as the standard access codes, and others which would be recognized as emergency codes. The comparison means of the computer system of the invention would be configured to accept and recognize at least one code per authorized user, and to activate the emergency alert means whenever the code entered by the user matched an emergency code. At the same time, the determination of an authorized identity for the user would result in the user being afforded access to the requested secured computer system perhaps on an access level that has been predetermined to be restricted or perhaps resulting in the display of misleading data (i.e., "false screens"), thereby preventing the coercing third party from knowing

5 that an emergency notification had been entered by the user. The
emergency code would be entered as a part of or simultaneously with the
user's personal identification code or by selecting an emergency account
index during the access of the computer system. In either case, the
well-being of the user requesting access might be jeopardized if the
coercing party discovered that the user was attempting to notify
authorities. Thus, it is critical that the access procedure continue
uninterruptedly and that access be granted to an authorized user so that the
coercing party believes that everything is proceeding normally. Although
10 these features can be incorporated into the invention's host computer
network, it is also possible that an independent computer network can also
carry out the same or modified versions of the above-mentioned features.

The present invention is clearly advantageous over the prior art
in a number of ways. First, it is extremely easy and efficient for the user,
15 particularly where the user is accessing financial accounts, because it
eliminates the need to carry and present any tokens in order to access one's
accounts. The present invention eliminates all the inconveniences
associated with carrying, safeguarding and locating any desired tokens.
Further, because tokens are often specific to a particular computer system
20 that further requires remembering a secret code assigned to the particular
token, this invention eliminates all such tokens and thereby significantly
reduces the amount of memorization and diligence increasingly required of
consumers by providing access to all assets using only one personal
identification code. Thus, in a single, tokenless transaction, the consumer
25 can efficiently and securely conduct virtually any commercial exchange or
electronic message, from withdrawing cash from a bank account, to
authorization his agreement to the terms of a contract, to making a
purchase directly from television, to paying local property taxes. The
consumer is now uniquely empowered, by means of this invention, to
30 conveniently conduct his personal and/or professional electronic
transmissions and transactions at any time without dependence upon tokens
which may be stolen, lost or damaged.

The invention is clearly advantageous from a convenience
standpoint to retailers and financial institutions by making purchases and
35 other financial transactions less cumbersome and more spontaneous. The
paper work of financial transactions is significantly reduced as compared to

current systems, such as credit card purchase wherein separate receipts are generated for use by the credit card company, the merchant and the consumer. Such electronic transactions also save merchants and banks considerable time and expense by greatly reducing operational costs. Because the system of the invention is designed to provide a consumer with simultaneous direct access to all of his financial accounts, the need for transactions involving money, checks, commercial paper and the like will be greatly reduced, thereby reducing the cost of equipment and staff required to collect and account for such transactions. Further, the substantial manufacturing and distributing costs of issuing and reissuing credit cards, ATM cards, calling cards and the like will be eliminated, thereby providing further economic savings to merchants, banks, and ultimately to consumers. In fact, the system of the invention will likely spur economic growth since all of a consumer's electronic financial resources will be available at the mere input of his fingerprint or other biometrics.

The invention is markedly advantageous and superior to existing systems in being highly fraud resistant. As discussed above, present computer systems are inherently unreliable because they base determination of a user's identity on the physical presentation of a unique manufactured object along with, in some cases, information that the user knows. Unfortunately, both the token and information can be transferred to another, through loss, theft or by voluntary action of the authorized user. Thus, unless the loss or unintended transfer of these items is realized and reported by the authorized user, anyone possessing such items will be recognized by existing security systems as the authorized user to whom that token and information is assigned.

By contrast, the present invention virtually eliminates the risk of granting access to non-authorized users by determining user identity from an analysis of one or more of a user's unique, biometrics characteristics. Even in the very rare circumstance of coercion, where an authorized individual is coerced by a coercing party to access his accounts, the system anticipates an emergency account index, whereby the authorized user can alert authorities of the transgression without the knowledge of the coercing party.

5 The invention further enhances fraud resistance by maintaining authenticating data and carrying out the identity verification operations at a point in the system that is operationally isolated from the user requesting access, thereby preventing the user from acquiring copies of the authenticating data or from tampering with the verification process. Such a system is clearly superior to existing token-based systems wherein authenticating information, such as personal codes, is stored on and can be recovered from the token, and wherein the actual identity determination is potentially in operational contact with the user during the access process.

10 It is an object of the invention therefore to provide a computer access identification system that eliminates the need for a user to possess and present a physical object, such as a token, in order to initiate a system access request.

15 It is another object of the invention to provide a computer access identification system that is capable of verifying a user's identity, as opposed to verifying possession of proprietary objects and information.

It is yet another object of the invention to verify user identity based upon one or more unique characteristics physically personal to the user.

20 Yet another object of the invention is to provide a system of secured access that is practical, convenient, and easy use.

Still another object of the invention is to provide a system of secured access to a computer system that is highly resistant to fraudulent access attempts by non-authorized users.

25 Yet another object of the invention is to provide a computer access identification system that enables a user to notify authorities that a particular access request is being coerced by a third party without giving notice to said third party of the notification.

30 There is also a need for a computer access identification system that automatically restricts a user's transactional capabilities on the computer system according to a desired configuration provided by the user.

35 These and other advantages of the invention will become more fully apparent when the following detailed description of the invention is read in conjunction with the accompanying drawings.

Brief Description of the Drawings

FIG. 1 is a diagram of the system of the present invention;

FIG. 2 is a diagram of the Data Processing Center (DPC) and its internal data bases and execution modules;

FIG. 3 is a diagram of the retail point of sale terminal, the biometrics input apparatus and its components, and the interconnections between them;

FIG. 4 is a flow chart of the operation of the biometrics input apparatus and the terminal for generating a request packet;

FIG. 5 is a representational diagram of the request packet and the mandatory and optional data it contains;

FIG. 6 is a representational diagram of the response packet and the mandatory and optional data it contains;

FIG. 7 is a flow chart depicting the data encryption and sealing process at the biometrics input device;

FIG. 8 is a flow chart depicting the data decryption and counter party identification process at the DPC;

FIG. 9 is a flow chart depicting the data encryption and sealing process at the DPC;

FIG. 10 is a flow chart representing the registration of an individual during the registration process;

FIG. 11 is a flow chart representing the process of identification of the individual and returning a private code to the individual;

FIG. 12 is a flow chart of the skeleton of the processes that occur at the DPC and an execution step;

FIG. 13 is a flow chart of the emergency request and response process at the DPC;

FIG. 14 is a flow chart of the overall operation of retail transaction authorization execution at the DPC;

FIG. 15 is a flow chart of the overall operation of remote transaction authorization execution step at the DPC;

FIG. 16 is a flow chart of the overall operation of ATM account access execution at the DPC;

FIG. 17 is a flow chart of the overall operation of issuer batch modification execution at the DPC;

FIG. 18 is a flow chart of the overall operation of secure fax submit and electronic document submit execution at the DPC;

FIG. 19 is a flow chart of the overall operation of secure fax data and electronic document data execution at the DPC;

FIG. 20A is a representational diagram of the electronic signature request packet;

FIG. 20B is a representational diagram of the electronic signature response packet;

FIG. 20C is a representational diagram of the electronic signature verification request packet;

FIG. 20D is a representational diagram of the electronic signature verification request packet;

FIG. 21 is a flow chart of the overall operation of electronic signature execution at the DPC; and

FIG. 22 is a flow chart of the overall operation of electronic signature verification execution at the DPC.

Detailed Description of the Drawings

As noted, the main objective of this invention is to provide a tokenless, secure, reliable, safe, and consistent, apparatus and method, for identifying individuals for the purpose of performing financial transactions and non-financial transmissions, which can accommodate large numbers of users. It is the essence of this invention that consumers have the ability to conduct these transactions without the use of any tokens, credit cards, badges or identification cards including drivers licenses. In order to be functional it is important that the system operate at speeds required for completing financial transactions such as credit card purchases and ATM services, from multiple banks and credit accounts. The system must be secure, such that individuals records and their biometrics information remain confidential and safe, both within the computer system that identifies the individual and authorizes transactions, or during transfer of data between the computer system and remote sites with which the computer system communicates. Furthermore, the system must be reliable

in that errors in identification and authorization must not hamper or make use of the system cumbersome. Since only the use of biometrics are contemplated for identification of individuals, the system must also have security measures to either reduce access, even to the authorized user, or notify authorities in emergency cases. It is appreciated that the system must be able to handle a large number of users, and accommodate storage and transfer of large amounts of data, such as bio-characteristic information, commensurate with speeds at which financial transactions are carried on today.

Turning now to the figures, the overall configuration of the invention and its components are shown in FIG. 1. Essentially a Data Processing Center (DPC) 1 is connected to various terminals 2 through various type of communication means 3 which can be one of several types. The DPC is also connected and communicates with independent computer networks 4. The DPC contains several data bases and software execution modules as shown in FIG. 2. In a preferred embodiment of the invention, the data bases are backed up or "mirrored" for safety reasons. The Firewall Machine 5 is responsible for prevention of electronic intrusion of the system while the Gateway Machine 6 is responsible for carrying out all requests from the user, including adding, deleting and otherwise modifying all data bases. The Gateway Machine is also responsible for decryption and de-packaging of data that has arrived from the terminals using the MACM module 7, MDM module 8, and the SNM module 9. The PGL module 10, and the IML module 11 are used to locate the proper personal identification code and biometrics sample basket. FIG. 3 depicts an example of a terminal and the biometrics input device 12, which has a biometrics scanner 13, data entry means such as a key pad or PIN pad 14, and a display panel 15. The biometrics scanner can be any one of finger print scanner, voice recognition, palm print scanner, retinal scanner or the like, although the fingerprint scanner will be used as an example. The biometrics input device is further equipped with computing modules 16, device drivers, and erasable and non-erasable memory modules. The biometrics input device communicates with the terminal through preferably a serial port 17. The terminal 2 communicates through a conventional modem 18 with the DPC 1 through request packets 19 and response packets 20 using one of the interconnecting means in FIG. 1 such as cable

network, cellular telephone networks, telephone networks, Internet, ATM network, or X.25. FIG. 4 shows a representational diagram of the request packet 19 and its method of generation by the biometrics input device software. FIG. 5 and FIG. 6 show a representational diagram of the request packet and response packet with optional and mandatory data segments. Furthermore, it is shown which parts of the packets are encrypted and which ones are sealed. FIG. 7 is a block diagram of the overall process for data encryption and sealing showing the use of DUKPT key data 20 for encryption of data before appending additional data before sealing the request packet with a Message Authentication Code Key (MAC) 21. FIG. 8 and FIG. 9 show the decryption and encryption process at the DPC. FIG. 12 through 19 and 21 through 22 are block diagrams of selected examples of execution steps carried on at the DPC.

Description of the drawings, diagrams, flow charts and the description of the invention, including hardware components, software components, execution modules, data bases, connection means, the data transferred between them, and the method of the invention is described in detail as follows.

1.1. Biometric Input Apparatus (BIA)

1.1.1. Introduction

The BIA is a combination of hardware and software whose job is to gather, encode, and encrypt biometric input for use in individual identification. All actions of the BIA are directed by an outside controlling entity called a terminal, which issues commands and receives results over the BIA's serial line.

BIA hardware comes in four basic versions: standard, wireless, integrated phone/cable television (or "CATV")/fax, and ATM. Each BIA hardware variant addresses a particular need in the marketplace, and because of the differences in construction, each variant has a different level of security.

BIA software comes in seven basic versions: personal computer (or "PC"), retail, ATM, registration, internal, issuer, and integrated remote. Each software load provides a different, use-specific command set. For

instance, the registration software load does not accept requests to form retail transaction messages. Likewise, the retail software command set cannot send individual registration messages. To provide another layer of security, the DPC knows what software package is loaded into each BIA; any attempts by an BIA to send a message that it is normally not able to send is rejected, and treated as a major security violation.

The ability of the invention to detect and combat merchant-based fraud relies on the fact that the BIA's external interface is strictly limited, that the construction of the BIA makes it extremely difficult to tamper with the contents, that each BIA has its unique encryption codes that are known only to the DPC, and that each BIA is only allowed to perform operations limited to its designated function. Each biometric input means has a hardware identification code previously registered with the DPC, which makes the biometric input means uniquely identifiable to the DPC in each subsequent transmission from that biometric input device.

The BIA is constructed with the assumption that the controlling terminal is a source for fraud and deception. Terminals range from software applications running on personal computers to dedicated hardware/software systems developed for a particular use such as a retail point of sale. Regardless of the particular model, no BIA reveals unencrypted biometric information. BIA models without display means (such as LCD, LED, or quartz screens) must reveal selected information (such as individual private codes) to the terminal for display, and as a result those particular terminal-BIA combinations are considered to be less secure.

Depending on the task at hand, BIA models are either partially or fully integrated with the terminal. Partially integrated devices are physically separate from the terminal, and they include wireless and standard retail point of sale BIAs. Fully integrated devices are contained within the physical enclosure of the terminal itself, for instance, an ATM, or a telephone.

No BIA ever discloses any secret encryption codes to any external source.

1.1.2. BIA Models

Particular BIA hardware models have different configurations. They are introduced in brief here:

BIA

Standard model has computing module (i.e., multichip modules), biometric scanner (i.e., single fingerprint scanner), display means (i.e., LCD screen), communications port (i.e., serial port), data entry means (i.e., a manual data entry key board or PIC pad) encased in tamper-resistant case, and electronic detection means (i.e., RF shielding).

BIA/Wireless

Standard model, but serial line replaced with spread-spectrum wireless communications module using external antenna. Used in restaurant point of sale.

BIA/ATM

Has heavy-duty scanner and serial port, along with a multichip module. The fact that the LCD is part of the terminal and not the BIA means lower security because it must reveal the private code to the terminal. Used in ATMs.

BIA/Catv

Has light-duty scanner, otherwise like ATM. Used in telephones, CATV remotes, and fax machines. Weakest security, both because the LCD and PIC pad are part of the terminal not the BIA, and because of the low-cost nature of the market.

1.1.3. BIA Command Set Messages

Each BIA software command set provides a different set of operations. They are introduced briefly here:

BIA/ATM

Account Access

BIA/Catv

Remote Transaction Authorization

BIA/Fax

- Secure Fax Submit
- Secure Fax Data
- Secure Fax Tracking
- Secure Fax Retrieve
- Secure Fax Reject
- Secure Fax Archive
- Secure Fax Contract Accept
- Secure Fax Contract Reject
- Electronic Document Archive Retrieve

BIA/Internal

Individual Identification

BIA/Issuer

Issuer Batch

BIA/PC

- Electronic Document Submit
- Electronic Document Data
- Electronic Document Tracking
- Electronic Document Retrieve
- Electronic Document Reject
- Electronic Document Archive
- Electronic Document Archive Retrieve
- Electronic Signature Submission
- Electronic Signature Check
- Remote Transaction Authorization
- Network Credential
- Secured Connection

BIA/Registration

Individual Identification

Biometric Registration

5

BIA/Retail

Transaction Authorization

1.1.4. BIA Hardware: Standard Model

10

The Standard BIA hardware is a multichip module combined with a single-print scanner, an LCD screen, a serial port, and a PIC pad encased in a hard tamper-resistant case that makes attempts to penetrate obvious while also providing RF shielding for the contents.

15

The following components are amalgamated into a multichip module, called the BIA Multichip Module (a process for encapsulating several processors in one physical shell, well known in the industry), constructed to protect the communications pathways between the devices from easy wiretapping.

20

- Serial processor
- PIC pad processor
- LCD screen processor
- CCD scanner A/D processor
- High-speed DSP processor containing both flash and mask ROM
- General purpose microprocessor
- Standard RAM
- EEPROM

25

30

The following software packages and data are stored in mask ROM. Mask ROM is cheaper than other types of read only memory, but it is easily reverse engineered, and is not electronically erasable. As such we only place the noncritical commonly available code here. (Mask ROM is well known in the industry).

35

- MAC calculation library
- DUKPT Key Management library
- DES (with CBC) Encryption library
- Base-64 (8-bit to printable ASCII) converter library
- Public Key Encryption library
- Embedded Operating System
- Serial line device driver
- LCD device driver
- PIC pad device driver
- Scanner device driver
- Unique hardware identification code
- Multi-Language profiles

The following standard data and software packages are stored in flash ROM. Flash ROM is more expensive, but it is much more difficult to reverse engineer, and most importantly, it is electronically erasable. All of the more critical information is stored here. Flash ROM is used in an attempt to increase the difficulty of duplicating an BIA. (Flash ROM is well known in the industry).

- Unique DUKPT Future Key Table
- Unique 112-bit MAC Key
- DSP biometric quality determination algorithm
- DSP biometric encoding algorithm
- Random number generator algorithm
- Command function table

The message sequence number, incremented each time a message is sent from the BIA, is stored in the EEPROM. EEPROM can be erased many times, but is also nonvolatile — its contents remain valid across power interruptions. (EEPROM is well known in the industry).

The following data is stored in RAM. RAM is temporary in nature, and is lost whenever power is lost.

- Encoded Biometric Register
- PIC Register

- Account Index Code Register
- Title Index Code Register
- Amount Register
- Document Name Register
- 5 • PIC-Block Key
- Message Key
- Response Key
- Shared Session Key
- Private Session Key
- 10 • 8 General Registers
- stack and heap space

Each multichip module contains a "write-once" memory location that is irreversibly set following the initialization of the flash ROM. Whenever an attempt is made to download software to the flash ROM, this memory location is checked; if it is already been set, then the BIA refuses to load. This way, critical software and data keys may only be downloaded once into the device, at the time of manufacture.

All registers and keys are explicitly zeroed when a transaction is canceled. Once a transaction is completed, registers are cleared as well. Once a "form message" command is executed, biometric, PIC, and account index code registers are also cleared, along with any encryption keys that aren't required for subsequent use.

It is important that the software not keep copies of registers or keys in stack variables (known in the industry).

The following associated hardware components comprise the standard BIA hardware module.

- 30 • BIA Multichip module
- CCD single-print scanner
- capacitance detector plate (known in the industry)
- lighted PIC keypad
- 2-line 40-column LCD screen
- 35 • RF shielding
- tamper-resistant case

- serial connection (up to 57.6kb)
- breach detection hardware (known in the industry)
- optional thermite charge attached to Multichip module (known in the industry)

5
10
All temporary storage and internal hardware and software used to calculate these values are secured, which means they resist any attempts to determine their current values, or their means of functioning. This feature is essential for the security of the invention, just as it is critical that the "wiretapping" of an BIA and specifically the gathering of a Biometric-PIC Block for fraudulent means is made as difficult as possible.

The multichip module and the components are, where practical, physically connected to each other without exposed wiring being present.

15
20
The enclosure protecting the electronic components of the BIA is welded shut during manufacture; it cannot be opened under any circumstances without significant damage to the case. Upon detecting any opening (or damage) of the enclosure, the BIA performs an emergency electronic zero of any and all keys residing in flash ROM, followed by all of the software libraries. Specific breach detection methods are kept confidential and proprietary.

In addition to protecting the contents, the case also shields the internal operations from RF signal detectors.

25
Supersecure versions of the BIA exist whereby breach detection methods are connected to a mechanism that physically destroys the multichip module as well as the detection methods themselves.

1.1.5. BIA Hardware: Wireless Model

30
The Wireless version of BIA hardware is identical to the Standard model in construction, except that it exports a spread-spectrum wireless communications module using an external antenna instead of an external serial port.

This version is designed to be used in restaurants, where transactions are authorized at the customer's convenience.

In the following descriptions, items which are added to the standard set are signified by the + character, while items that are removed from the standard set are signified by the - character.

5

Multichip Module:

- Document Name Register
- Shared Session Key
- Private Session Key
- Message Key

10

Components:

- Serial port
- + External antenna
- + Spread-spectrum wireless serial module (known in the industry)

15

1.1.6. BIA Hardware: ATM Model

20

The ATM version of BIA hardware is a multichip module combined with a heavy-duty single-print scanner and a serial port. The components are encased in a tamper-resistant case that makes attempts to penetrate obvious while also providing RF shielding for the contents.

25

This version is designed to be retrofitted into ATM locations. As such, the scanner pad is a heavy-duty sensor pad, and the entire construction makes use of the existing screens and keypads present in the ATM itself.

30

In the following descriptions, items which are added to the standard set are signified by the + character, while items that are removed from the standard set are signified by the - character.

Multichip Module:

- Amount Register
- Document Name Register
- Shared Session Key
- Private Session Key
- Message Key

35

Components:

- lighted PIC keypad
- 2-line 40-column LCD screen

5 Note that since the ATM has no LCD screen or PIC keypad, it really has no need of those device drivers in the mask ROM.

1.1.7. BIA Hardware: Phone/CATV Model

10 The Phone/CATV version of BIA hardware is a multichip module combined with a single-print scanner and a serial port. The module is physically attached to the scanner, and the whole is encased in plastic in order to make tampering more difficult. Some amount of RF shielding is provided for the components.

15 This version is designed to be integrated with telephones, television remote controls, and fax machines. As a result, it makes use of the existing keypads and LCD or television screens to enter or display values. It also uses the communication facilities of the host terminal. For example, the fax machine uses the built-in fax modem and the television remote uses the CATV cable network.

20 This hardware model is (in comparison with other models) relatively insecure, as it is intended that these devices cost as little as possible, be lightweight, and integrate easily with existing low-cost devices.

25 Of course, higher-security versions with more complete enclosures are possible and encouraged.

30 In the following descriptions, items which are added to the standard set are signified by the + character, while items that are removed from the standard set are signified by the - character.

Multichip Module:

- Document Name Register
- Shared Session Key
- Private Session Key
- Message Key

Components:

- lighted PIC keypad
- 2-line 40-column LCD screen

1.2. BIA Software**1.2.1. BIA Software Command Interface:**

The external interface to the BIA is much like a standard modem; commands are sent to it from a controlling terminal using the external serial line. When a command completes, a response code is sent from the BIA to the terminal.

Each BIA software load supports a different set of operations. For instance, a retail load supports only transaction authorizations, while a registration load supports individual identification and biometric registration.

All BIA data fields are in printable ASCII, with fields separated by field separator (or "fs") control character, and records separated by newlines. Encrypted fields are binary converted to 64-bit ASCII using the base-64 conversion library (all known in the industry).

Some commands are not available in some configurations. For instance, the ATM BIA cannot "Get PIC", since there is no attached PIC pad. Instead, the ATM BIA supports a "Set PIC" command.

Response Codes:**Out of time:**

The time allotted for the command has expired. A message to that effect will be displayed on the LCD screen, if available. When time expires for a given command, the BIA acts as if the cancel button was pushed.

Canceled:

The "cancel" button has been pushed, and the entire operation has been canceled. This has the side effect of clearing all information

which was gathered. A message to that effect will be displayed on the LCD screen, if available.

Ok:

The command was successful.

Other:

Each command may have specific other response codes which are valid only for it. These response codes will generally have text accompanying the code, which will be displayed on the LCD screen if it is available.

Message:

This indicates that the command is ongoing, but that the BIA wants to send a message to the terminal with an interim result message. The result is also displayed on the LCD, if available. This facility is used for prompts, as well as status messages.

Commands:

In the argument list of the commands below, the <> characters surround individual arguments, [] characters surround optional arguments, and the | character indicates that a given argument may be comprised of one of the choices presented.

Set Language <language-name>

This command selects from one of a number of different languages encoded within the BIA for prompting for user input.

Get Biometric <time> [primary|secondary]

This command requests the BIA to activate its scanner to get biometric input from the individual, storing it into the Encoded Biometric Register.

First, the message "Please place finger on lighted panel" is displayed on the LCD panel and returned to the terminal. The scanner pad is illuminated, prompting the individual to enter his biometric.

A <time> value of zero means that there is no limit to the time for biometric scan input.

When in scanning mode, a fingerprint scan is taken and given a preliminary analysis by the print quality algorithm. If the scan is not good enough, the BIA continues to take new scans until <time> seconds pass. As time passes and snapshots of the print are taken and analyzed, messages are posted to the LCD screen and sent to the terminal based on the problems detected by the print quality software. If no print of appropriate quality is forthcoming, the BIA returns an error code of time expired, displaying a message to that effect on the LCD.

Once the print quality algorithm affirms the quality of the print scan, the print's minutiae are then extracted by the print encoding algorithm. Only a subset of the minutiae are selected at random, with care taken to retain enough sufficient for identification. These minutiae are then ordered randomly, and are placed in the Encoded Biometric Register. Then the BIA responds with the success result code.

If the [primary|secondary] is specified (only available in the biometric registration command set) then the entire minutiae set is selected, not just the smaller subset. Likewise, primary/secondary biometric selection ends up placing the encoded biometric into the appropriate register.

Whether or not the operation succeeds, as soon as scanning has terminated, the light indicating that scanning is in progress is turned off.

It is very important that the same biometric input yields different encodings, so as to complicate the task of anyone attempting to discover the encryption codes of a captured BIA. This is accomplished by the selection of a random subset and random ordering of the encoded biometric.

Get PIC <time>

This command requests the BIA to fill the PIC Register by reading from the keypad.

First, the message "Please enter your PIC, then press <enter>" is displayed on the LCD display and sent to the terminal, the appropriate keypad lights are turned on, and then keypad scanning begins.

Scanning terminates when either <time> number of seconds runs out, or when the individual hits the "enter" key.

Note that the individual digits of the PIC are not displayed on the LCD panel, but for each digit the individual types, a star "*" appears to give the individual feedback. When the "correction" key is pressed, the last digit entered is erased, allowing the individual to fix input mistakes.

When PIC input terminates, the keypad lights turns off.

If successful, the command returns OK.

Get Account Index Code <time>

First, the message "Now enter your account index code, then press <enter>" is displayed on the LCD and sent to the terminal. This prompts the individual to enter his account index code. When each key is pressed, that value appears on the LCD panel. The correction button can be pressed to erase one of the values. When the "enter" button is pressed, the Account index code register is set.

During input, the appropriate keypad keys are lit, and when input is concluded, the keypad lights are turned off.

If successful, the command returns OK.

Get Title Index Code <time>

First, the message "Please enter your title index code, then press <enter>" is displayed on the LCD and sent to the terminal. This prompts the individual to enter his title index code. When each key is pressed, that value appears on the LCD panel. The correction button can be pressed to erase one of the values. When the "enter" button is pressed, the Title Index Code register is set.

During input, the appropriate keypad keys are lit, and when input is concluded, the keypad lights are turned off.

If successful, the command returns OK.

Validate Amount <amount> <time>

The Validate Amount command sends the message "Amount <amount> OK?" to the terminal, and displays it on the LCD screen. If the individual confirms the amount by hitting the "yes" (or enter) button, the Amount Register is set to <amount>. The <amount> value must be a valid number,

with no control characters or spaces, etc. During prompting, the yes, no, and cancel buttons are lit. Once prompting is complete, all the lights are turned off.

If the individual enters "no", then the transaction is canceled.

Enter Amount <time>

The Enter Amount command sends the message "Enter amount" to the terminal, and also displays it on the LCD screen as well. The individual must then enter the dollar amount himself. Each character entered is displayed on the LCD screen. All appropriate buttons are lit. If the enter button is hit, the Amount Register is set to be the value entered on the keyboard. Once entry is complete, all the lights are turned off.

Validate Document <name> <time>

The Validate Document command sends the message "Document <name> OK?" to the terminal, and displays it on the LCD screen as well. If the individual confirms the document by hitting the "yes" (or enter) button, the Document Name Register is set to <name>. The <name> must be printable ASCII, with no control characters, and no leading or trailing spaces. During prompting, the yes, no, and cancel buttons are lit. Once prompting is complete, all the lights are turned off.

If the individual enters "no", the transaction is canceled.

Assign Register <register> <text>

The assign register command sets the designated General <register> to have the value <text>. This is used to set information such as the merchant code, the product information, and so on.

Get Message Key

The Get Message Key command causes the BIA to generate a 56-bit random key to be used by the controlling hardware to encrypt any message body that the controlling device wishes to add to the message. That generated key is returned by the BIA in hexadecimal format (known in the industry). The message key are then added to the biometric-PIC block.

Form Message <type=identification|transaction|account access...>

The form message command instructs the BIA to output a message containing all the information it has gathered. It also checks to make sure that all the registers appropriate to that specific message <type> have been set. If all required registers are not set, the BIA returns with an error. The specific command set software will determine which messages can be formed by that BIA model; all others will be rejected.

Each message includes a transmission code consisting of the BIA's unique hardware identification code and an incrementing sequence number. The transmission code allows the DPC to identify the sending BIA and to detect resubmission attacks.

The BIA uses the DUKPT key management system to select the biometric-PIC block encryption 56-bit DES key from the Future Key Table. This key is then used to encrypt the Biometric-PIC Block using cipher block chaining (CBC). In addition, a response DES key is also generated randomly, and is used by the DPC to encrypt the portions of the response that need to be encrypted.

Note: splitting the response key from the biometric-PIC block key is very important, since each encryption key must be used only within the context of its own responsibilities. That way, if someone were to break the key encoding the private code, it would not result in the disclosure of the biometric-PIC.

The Biometric-PIC block consists of the following fields:

300-byte authorization biometric

4-12 digit PIC

56-bit response key

[optional 56-bit message key]

Note that the message key is only present if the controlling terminal has requested a message key for this message. It is up to the controlling terminal to encrypt any message body attached to the transaction authorization request using the message key.

Once all encryption is complete, the BIA outputs the body of the appropriate request message (such as a Transaction Authorization

Request message), terminated by and protected with the Message Authentication Code (MAC).

5 The MAC field is calculated using the BIA's secret 112-bit DES MAC key, and covers all message fields from first to last. The MAC assures the DPC that nothing in the message has changed effectively sealing the message, while still allowing the plaintext fields to be inspected by the controlling terminal.

10 When the Form Message command is done, the BIA sends the message "I'm talking to DPC Central" to the terminal as well as displaying it on the LCD screen, indicating that work is proceeding on the request.

The command returns OK in addition to returning the entire formed message upon completion of the command.

Show Response <encrypted response> <time>

15 The Show Response command instructs the BIA to use its current Response Key to decrypt the private code from the system.

20 After decryption, a chime sounds, and the private code is displayed on the LCD screen for <time> seconds. At no time does this command transmit the decrypted private code to the controlling terminal.

Validate Private <encrypted validation> <time>

25 This command is used by a terminal during a secure network communications session to ask the individual to validate a message from an outside source. The message comes encrypted and in two parts: the challenge, and the response.

30 Upon receipt of a Validate Private command, the BIA displays the text of the challenge message as in "OK <challenge>?" on the LCD screen, but does not send this to the terminal. When the individual validates the challenge, the response is encrypted by the BIA using the Private Session Key, and then returned to the terminal along with the OK response code. If the individual does not validate the challenge, then the BIA returns with a "failed" response code, along with the text "transaction canceled at your request," which is also displayed on the LCD screen.

35 Note that the terminal is never allowed to see the plaintext of either the challenge or the response.

Reset

The Reset command instructs the BIA to clear all temporary registers, the LCD screen, all temporary Key registers, and to turn off all keypad lights that may be on.

5

Set PIC <value>

This command assigns the BIA's PIC Register to be <value>.

Note that allowing a non-secured device to provide the PIC is a potential security problem, because non-secured devices are much more vulnerable to wiretapping or replacement.

10

Set Account index code <value>

This command assigns the BIA's Account index code Register to be <value>.

15

Note that allowing a non-secured device to provide the account index code is a potential security problem, because non-secured devices are much more vulnerable to wiretapping or replacement.

20

Set Title Index Code <value>

This command assigns the BIA's Title Index Code Register to be <value>.

Note that allowing a non-secured device to provide the Title Index Code is a potential security problem, because non-secured devices are much more vulnerable to wiretapping or replacement.

25

Set Amount <value>

This command assigns the BIA's Amount Register to be <value>.

30

Decrypt Response <encrypted response message>

The Decrypt Response command instructs the BIA to use its current Response Key to decrypt the encrypted portion of the response message. Once decrypted, the response is returned to the controlling device, presumably for display on the ATM terminal's LED screen.

35

Note that providing this decryption ability is a security problem, as once the plaintext leaves the BIA, the terminal has the ability to do with it what it will.

1.2.2. BIA Software: Support Libraries

The BIA software is supported by several different software libraries. Some of them are standard, generally available libraries, but some have special requirements in the context of the BIA.

1.2.2.1. Random Number Generator

Since the BIA is constantly selecting random DES keys for use in the message body and message response encryption, it is important that the keys selected be unpredictable keys. If the random number generator is based on time of day, or on some other externally-predictable mechanism, then the encryption keys will be much more easily guessed by an adversary that happens to know the algorithm. In order to assure the security of the encryption techniques used in the BIA, it is assumed that both the random number generator algorithm as well as the encryption algorithms are both publicly known.

A standard random number algorithm for generating DES keys is defined in ANSI X9.17, appendix C (known in the industry).

1.2.2.2. DSP Biometric Encoding Algorithms

The biometric encoding algorithm is a proprietary algorithm for locating the minutiae that are formed by ridge endings and bifurcations on human fingertips. A complete list of minutiae is stored in the DPC as a reference, while only a partial list is required by the algorithm when performing a comparison between an identification candidate and a registered individual.

During both biometric registration as well as identification, the encoding algorithm ensures that enough minutiae are found before ending the biometric input step.

1.2.2.3. Operating System and Device Drivers

5 The BIA is a realtime computing environment, and as such requires a realtime embedded operating system to run it. The operating system is responsible for taking interrupts from devices and scheduling tasks.

10 Each device driver is responsible for the interface between the operating system and the specific hardware, such as the PIC pad device driver, or the CCD Scanner device driver. Hardware is the source for events such as "PIC pad key pressed", or "CCD Scanner scan complete". The device driver handles such interrupts, interprets the events, and then takes action on the events.

1.2.2.4. DES Encryption Library

15 There are any number of DES implementations publicly available. DES implementations provide a secret key-based encryption from plaintext to ciphertext, and decryption from ciphertext to plaintext, using 56-bit secret keys.

1.2.2.5. Public Key Encryption Library

25 Public Key encryption support libraries are available from Public Key Partners, holders of the RSA public key patent (known in the industry). Public Key cryptosystems are asymmetric encryption systems that allow communication to take place without requiring a costly exchange of secret keys. To use a public key encryption system, a public key is used to encrypt a DES key, and then the DES key is used to encrypt a message. The BIA uses public key cryptosystems to provide for the secure exchange of secret keys.

30 Unfortunately, public key systems are significantly less well tested than secret-key systems, and as such there is an overall lower level of confidence in such algorithms. As a result, the invention uses public key cryptography for communications security and short-lived credential exchange, and not long-term storage of secrets. Both the end-user
35 individual and the bank are identified by the DPC to create the network

credential. The network credential includes the end-user individual's identification as well as the context of the connection (i.e., the TCP/IP source and destination ports).

5 1.2.2.6. DUKPT Key Management Library

The derived unique key per transaction key (DUKPT) management library is used to create future DES keys given an initial key and a message sequence number. Future keys are stored in a Future Key Table. Once used, a given key is cleared from the table. Initial keys are only used to generate the initial future key table. Therefore the initial key is not stored by the BIA

10 The use of DUKPT is designed to create a key management mechanism that provided a different DES key for each transaction, without leaving behind the trace of the initial key. The implications of this are that even successful capture and dissection of a given future key table does not reveal messages that were previously sent, a very important goal when the effective lifetime of the information transmitted is decades. DUKPT is fully specified in ANSI X9.24 (known in the industry).

15 DUKPT was originally developed to support PIC encryption mechanisms for debit card transactions. In this environment, it was critical to protect all transactions. An assumption is made that a criminal records encrypted transactions for a six month period, and then captures and successfully extracts the encryption code from the PIC pad. The criminal could then manufacture one new counterfeit debit card for each message that had been transmitted over that six month period. Under DUKPT, however, the criminal's theft and dissection would not allow him to decrypt previous messages (although new messages would still be decryptable if the criminal were to replace the PIC pad subsequent to dissection).

20 In the biometric-PIC situation, the criminal has an even harder time, as even if messages are decrypted, turning a digital biometric-PIC into a physical fingerprint is much harder than turning an account number-PIC into a plastic card, which is one of the significant benefits of the tokenless system.

25 Still, if a criminal can decrypt, he can encrypt, which might allow him to electronically submit a biometric-PIC to the system to

authorize a fraudulent transaction. While this is quite difficult, it is still best to restrict the options available to the criminal as much as possible, hence the use of DUKPT.

5 **1.3. BIA Software Command Sets**

1.3.1. BIA Software: Retail Command Set

10 The BIA/Retail software interface exports an interface that allows specific retail point of sale terminals to interact with the system.

 The BIA/Retail interface is designed to allow the terminal to perform the following operation:

15 Transaction Authorization

 In order to implement those operations, the BIA/Retail provides the following command set:

- 20 Set Language <language-name>
 Get Biometric <time>
 Get PIC <time>
 Assign Register <register> <value>
 Get Account index code <time>
 25 Validate Amount <amount> <time>
 Enter Amount <time>
 Form Message <type>
 Show Response <encrypted response> <time>
 Reset

30 **1.3.2. BIA Software: CATV (Integrated Remote) Command Set**

 The BIA/CATV software interface exports a command set that allows terminals integrated with a Phone/CATV BIAs to interact with the system. The following operation is supported:

35 Remote Transaction Authorization

In order to implement that operation, the BIA/CATV provides the following command set:

5 Get Biometric <time>
 Set PIC <text>
 Assign Register <register> <text>
 Set Account index code <text>
 Form Message <type>
 10 Decrypt Response <encrypted response message>
 Reset

1.3.3. BIA Software: Integrated FAX Command Set

15 The BIA/Fax software interface exports a command set that allows terminals integrated with a fax BIA to interact with the system. The following operations are supported:

20 Secure Fax Submit
 Secure Fax Data
 Secure Fax Tracking
 Secure Fax Retrieve
 Secure Fax Reject
 Secure Fax Archive
 25 Secure Fax Contract Accept
 Secure Fax Contract Reject
 Electronic Document Archive Retrieve

30 In order to implement these operations, the BIA/Fax provides the following command set:

 Get Biometric <time>
 Set PIC <text>
 Set Title Index Code <text>
 35 Assign Register <register> <value>
 Get Message Key

Form Message <type>
 Decrypt Response <encrypted response message>
 Reset

5 1.3.4. BIA Software: Registration Command Set

The BIA/Reg software interface exports an interface that allows
 general purpose computers to interact with the system to identify and
 register individuals. The following operations are supported:

Individual Identification
 Biometric Registration

10 In order to support those operations, the BIA/Reg provides the
 following command set:

Set Language <language-name>
 Get Biometric <time> [primary|secondary]
 Get PIC <time>
 20 Assign Register <register> <text>
 Get Message Key
 Form Message <type>
 Show Response <encrypted response> <time>
 25 Reset

30 1.3.5. BIA Software: PC Command Set

The BIA/PC software interface exports a command set that
 allows general purpose computers to send, receive, and sign electronic
 documents, conduct transactions across the network, and provide
 biometric-derived credentials to sites on the network. The following
 operations are supported:

35 Electronic Document Submit
 Electronic Document Data
 Electronic Document Tracking

Electronic Document Retrieve
 Electronic Document Reject
 Electronic Document Archive
 Electronic Document Archive Retrieve
 Electronic Signature Submission
 Electronic Signature Check
 Remote Transaction Authorization
 Network Credential
 Secured Connection

In order to support those operations, the BIA/PC provides the following command set:

Set Language <language-name>
 Get Biometric <time>
 Get PIC <time>
 Get Account index code <time>
 Validate Amount <amount> <time>
 Enter Amount <time>
 Validate Document <name> <time>
 Assign Register <register> <text>
 Get Message Key
 Form Message <type>
 Show Response <encrypted response> <time>
 Validate Private <encrypted validation> <time>
 Reset

1.3.6. BIA Software: Issuer Command Set

The BIA/Iss software interface exports an interface that allows general purpose computers to interact with the system to authenticate and submit batch change requests. The following operation is supported:

Issuer Batch

In order to implement this operation, the BIA/Iss provides the following command set:

- Set Language <language-name>
- Get Biometric <time> [primary|secondary]
- Get PIC <time>
- Assign Register <register> <value>
- Get Message Key
- Form Message <type>
- Show Response <encrypted response> <time>
- Reset

1.3.7. BIA Software: Internal Command Set

The BIA/Int exports a command set that allows general purpose computers to interact with the system to identify individuals. The following operation is supported:

Individual Identification

In order to implement this operation, the BIA/Int provides the following command set:

- Set Language <language-name>
- Get Biometric <time>
- Get PIC <time>
- Assign Register <register> <value>
- Get Message Key
- Form Message <type>
- Show Response <encrypted response> <time>
- Reset

1.3.8. BIA Software: ATM Command Set

The BIA/ATM software interface exports a command set that allows ATMs to identify individuals. The following operation is supported:

Account Access

5 In order to implement this operation, the BIA/ATM provides the following command set:

Get Biometric <time>

Set PIC <text>

Set Account index code <text>

10 Assign Register <register> <value>

Form Message <type>

Decrypt Response <encrypted response message>

Reset

15 1.4. Terminals

1.4.1. Introduction

20 The terminal is the device that controls the BIA and connects to the DPC via modem, X.25 connection, or Internet connection — methods well-known to the industry. Terminals come in different shapes and sizes, and require different versions of the BIA to perform their tasks. Any electronic device, which issues commands to and receives results from the biometric input device, can be a terminal.

25 Some terminals are application programs that run on a general purpose microcomputer, while other terminals are combinations of special purpose hardware and software.

30 While the terminal is critical for the functioning of the system as a whole, the system itself places no trust in the terminal whatsoever. Whenever a terminal provides information to the system, the system always validates it in some manner, either through presentation to the individual for confirmation, or by cross-checking through other previously registered information.

35 While terminals are able to read some parts of BIA messages in order to validate that the data was processed properly by the BIA,

terminals cannot read biometric identification information including the biometric, the PIC, encryption keys, or account index codes.

Specific BIAs export some security functionality to the terminal, such as PIC entry, and private code display. As a result, such devices are regarded as somewhat less secure than their entirely self-contained counterparts, and as such have consequently lower security ratings.

There are many different terminal types; each is connected to a specific model BIA. Each terminal is described in brief below:

ATM (Automated Teller Machinery)

Integrated BIA/ATM with ATM software load provides biometric-PIC access to ATM cash dispensers.

BRT (Biometric Registration Terminal)

Standard BIA with Registration software load attached to a microcomputer provides banks with the ability to register new individuals with the system along with their financial asset accounts and other personal information.

CET (Certified Email Terminal)

Standard BIA with PC software load attached to a microcomputer provides individuals with the ability send, receive, archive, reject, and track certified email messages.

CPT (Cable-TV Point of Sale Terminal)

BIA/catv with CATV software load attached to the CATV broadband provides individuals with biometric-television (or "TV") remotes with the ability to authorize television shopping purchases.

CST (Customer Service Terminal)

Standard BIA with Internal software load attached to a microcomputer system authorizes employees to construct database requests for the purposes of customer service.

EST (Electronic Signature Terminal)

Standard BIA with personal computer software load attached to a microcomputer provides individuals with the ability to construct and verify electronic signatures on documents.

5

IPT (Internet Point of Sale Terminal)

Standard BIA with personal computer software load attached to a microcomputer provides individuals with internet connections the ability to purchase products from a merchant that is connected to the Internet.

10

IT (Issuer Terminal)

Standard BIA with Issuer software load attached to a microcomputer provides banks with the ability to send batched changes of asset accounts to the DPC.

15

ITT (Internet Teller Terminal)

Standard BIA with personal computer software load attached to a microcomputer with an internet connection provides individuals with the ability to perform transactions with their favorite Internet Bank.

20

PPT (Phone Point of Sale Terminal)

BIA/catv with CATV software load integrated with a telephone provides individuals with the ability to authorize transactions over the telephone.

25

RPT (Retail Point of Sale Terminal)

Standard BIA with Retail software load attached to an X.25 network or using a modem allows an individual to purchase items using transaction authorizations in a store.

30

SFT (Secure Fax Terminal)

BIA/catv with Fax software load integrated with a fax machine provides individuals with the ability to send, receive, reject archive, and track secured fax messages.

35

1.4.2. Terminal: Retail Point of Sale Terminal

1.4.2.1. Purpose

5 The purpose of the RPT is to allow individuals to purchase items at a store without having to use either cash, check, or a debit or credit card.

10 The RPT uses a BIA/Retail to authorize financial transactions from an individual to a merchant. In addition to being used to accept biometric-PIC authorizations, the RPT provides standard debit and credit card scanning functions as well.

15 Note that only the biometric-related transactions are described in detail here. It is assumed that the RPT will also consist of standard credit and debit magnetic stripe card readers, as well as optional smart card readers too.

1.4.2.2. Construction

20 Each RPT is connected to the DPC by a modem, an X.25 network connection, an ISDN connection, or similar mechanism. The RPT may also be connected to other devices, such as an electronic cash register, from which it obtains the amount of the transaction and the merchant code.

25 The RPT consists of:

- an BIA/Retail
- an inexpensive microprocessor
- 9.6 kb modem/X.25 network interface hardware
- merchant identification code number in non-volatile RAM
- a DTC serial port for connecting to the BIA
- 30 • magnetic stripe card reader (known in the industry)
- ECR (electronic cash register) connection port
- optional smart card reader (known in the industry)

1.4.2.3. Identification

Two entities need to be identified for the DPC to respond positively to an BIA transaction authorization request: the individual, and the merchant.

The individual is identified by the biometric-PIC, and the merchant is identified by the DPC, which cross-checks the merchant code contained in the BIA's VAD record with the merchant code added to the transaction request by the RPT.

1.4.2.4. Operation

First, the merchant enters the value of the transaction into his electronic cash register. Then, the individual enters his biometric-PIC, his account index code, and then validates the amount. The RPT then adds the product information and the merchant code to the BIA, instructs the BIA to construct the transaction, and then sends the transaction to the DPC through its network connection (modem, X.25, etc).

When the DPC receives this message, it validates the biometric-PIC, obtains the account number using the index code, and cross-checks the merchant code in the message with the registered owner of the BIA. If everything checks out, the DPC forms and sends a credit/debit transaction to execute the exchange. The response from the credit/debit network is added to the private code to form the transaction response message, which the DPC then sends back to the RPT. The RPT examines the response to see whether or not the authorization succeeded, and then forwards the response to the BIA, which then displays the individual's private code, concluding the transaction.

1.4.2.5. Security

Messages between the RPT and the DPC are secured by encryption and MAC calculation from the BIA. The MAC allows the RPT to review the unencrypted parts of the message, but the RPT cannot change them. Encryption prevents the encrypted part of the message from being disclosed to the RPT.

Each retail BIA must be registered to a merchant. This helps to discourage BIA theft. Furthermore, because the RPT adds the merchant code onto each message, replacing a merchant's BIA with a different BIA is detected by the cross-check performed at the DPC.

1.4.3. Terminal: Internet Point of Sale Terminal

1.4.3.1. Purpose

The purpose of an Internet Point of sale Terminal (IPT) is to authorize credit and debit financial transactions from an individual at a computer to a merchant, both of whom are on the Internet.

Note that the Internet simply represents a general purpose network where a merchant, the DPC, and the IPT can all connect to each other in real time. As a result, this mechanism would work exactly the same on any other general purpose network.

1.4.3.2. Construction

The IPT consists of:

- an BIA/PC
- a microcomputer
- an Internet Shopper software application
- an Internet (or other network) connection

1.4.3.3. Identification

In addition to identifying the individual, the IPT must also identify the remote merchant who is the counterparty to the transaction. The merchant must also identify both the DPC and the IPT.

The Internet Shopper program stores the hostname (or other form of net name) of the merchant from which the purchase is taking place in order to verify the merchant's identity. Since the merchant registers all of his legitimate internet hosts with the DPC, this allows the DPC to cross-check the merchant code with the merchant code stored under that hostname to verify the merchant's identity.

1.4.3.4. Operation

First, the IPT connects to the merchant using the Internet.

5 Once a connection is established, the IPT secures it by generating and then sending a Session Key to the merchant. In order to assure that the session key is protected from disclosure, it is encrypted with the merchant's Public Key using Public Key Encryption. When the merchant receives this encrypted Session Key, he decrypts it using his Private Key. This process is called securing a connection through a Public Key Encrypted secret key exchange.

10 Once connected, the IPT downloads the merchant code, and both price and product information from the merchant. Once the individual is ready to make a purchase, he selects the merchandise he wishes to buy. Then, the individual enters the biometric-PIC using the BIA/PC, the IPT sends the merchant code, the product identification information, and the amount to the BIA, and instructs it to construct a Remote Transaction Authorization request. Then the IPT sends the request to the merchant via the secure channel.

15 The merchant is connected to the DPC via the same sort of secure connection that the IPT has with the merchant, namely, using Public Key Encryption to send a secure session key. Unlike the IPT-merchant connection, however, merchant-DPC session keys are good for an entire day, not for just one connection.

20 The merchant connects to the DPC, securing the connection using the session key, forwarding the transaction to the DPC for validation. The DPC validates the biometric-PIC, cross-checks the merchant code contained in the request with the merchant code stored under the hostname that was sent in the request, and then sends a transaction to the credit/debit network. Once the credit/debit network responds, the DPC constructs a reply message including the credit/debit authorization, an encrypted private code, and the address of the individual, and sends that message back to the merchant.

25 The merchant receives the reply, it copies the individual's mailing address out of the reply, makes note of the authorization code, and forwards the reply message to the IPT.

The IPT hands the reply to the BIA, which decrypts the private code and displays it on the LCD screen, indicating that the DPC recognized the individual. The IPT also shows the result of the transaction as well, be it success or failure.

1.4.3.5. Security

Since the system in general assumes that an adversary inhabiting the network can hijack network connections at any point, all parties must have secure communications during their realtime interactions. The main concern isn't disclosure of information, but rather insertion or redirection of messages.

The whole system of Public Key Encryption relies on having a trusted source for the Public Keys. These trusted sources are called Certifying Authorities, and we assume that such a source will be available on the Internet in the near future.

1.4.4. Terminal: Internet Teller Terminal

1.4.4.1. Purpose

The Internet Teller Terminal (ITT) is used to identify individuals for internet banking sessions. The DPC, the bank's computer system, and the individual are all connected to the Internet.

There are two main tasks. The first is providing a secure communications channel from the ITT to an internet bank. The second is providing unimpeachable identity credentials to the internet bank. Once both are accomplished, the ITT can provide a secure internet banking session. In addition, the BIA's challenge-response verification capability is used to provide additional security for all high-value and/or irregular transactions.

1.4.4.2. Construction

The ITT consists of:

- an BIA (standard PC model)
- a microcomputer
- an Internet Teller software application
- an Internet connection

The ITT accepts biometric identification using an BIA/PC connected to the microcomputer serving as the individual's Internet terminal.

1.4.4.3. Identification

Both the individual and the bank are identified by the DPC to create the network credential. The network credential includes the individual's identification as well as the context of the connection (i.e., the TCP/IP source and destination ports).

The DPC identifies the bank by cross-checking the code that the bank sends to the ITT with the bank's hostname that the ITT sends to the DPC.

1.4.4.4. Operation

First, the ITT connects to the internet bank, making sure that the bank has the computing resources required to handle a new session for the individual. If the bank has sufficient resources, it sends back the bank identification code to the ITT.

Once connected, the ITT instructs the BIA to obtain the biometric-PIC and the account index code from the individual. Then the ITT adds both the bank's hostname as well as the bank code. Using all this information, the BIA is then asked to form a network credential request message which the ITT sends to the DPC via the Internet.

When the DPC receives this message, it validates the biometric-PIC, obtains the account number using the index code, and makes sure that the bank code from the message matches the bank code stored under the

5 bank's hostname in the Remote Merchant database. The DPC also checks to make sure that the account number returned by the index code belongs to the bank as well. If all checks out, then the DPC creates a network credential using the individual's account identification, the time of day, and the bank code. The DPC signs this credential using Public Key Encryption and the DPC's Private Key. The DPC retrieves the bank's public key, and the individual's private code, and with the credential forms the network credential response message. The response message is encrypted using the BIA response key, and is then sent back to the ITT.

10 When the ITT receives the response, it hands the response message to the BIA. The BIA decrypts and then displays the individual's private code on the LCD screen. The bank's public key is stored in the Public Key register. Two random session keys are generated by the BIA. The first key, called the Shared Session Key, is revealed in plaintext to the ITT. The ITT uses this shared session key to secure the connection with the bank.

15 The other session key, called the Private Session Key, is not shared with the ITT. It is used for the BIA's challenge-response mechanism, a mechanism that allows the bank to obtain specific validation for non-routine transactions straight from the individual, without involving the (untrustworthy) ITT.

20 After receiving the Shared Session Key, the ITT asks the BIA to form a Secure Connection Request message, which includes both session keys and the network credential, and are all encrypted with the bank's public key. The ITT then sends the Secure Connection Request message to the bank.

25 When the bank receives the request message, it decrypts the message using its own Private Key. Then, it decrypts the actual network credential using the DPC's public key. If the network credential is valid and has not expired (a credential times out after a certain number of minutes), the individual is authorized, and the conversation continues, with the session key used to ensure security.

30 Whenever the individual performs any non-routine or high-value transactions, the bank may wish to ask the individual to validate those transactions for extra security. To do so, the bank sends a challenge-response message encrypted with the Private Session Key to the
35

ITT, which forwards that challenge-response message to the BIA. The BIA decrypts the message, displays the challenge (usually of the form "Transfer of \$2031.23 to Rick Adams OK?"), and when the individual validates by hitting the OK button, the BIA re-encrypts the response with the Private Session Key and sends that message to the ITT, which forwards it to the bank, validating the transaction.

1.4.4.5. Security

The system makes use of public key cryptography to both provide credentials and to secure communications between the ITT and the bank.

For this mechanism to function properly, the bank must know the DPC's public key, and the DPC must know the bank's public key. It is critical to the security of the system that both parties keep the respective public keys secure from unauthorized modification. Note that public keys are readable by anyone, they just cannot be modifiable by anyone. Of course, any session or secret keys must be kept secure from observation, and those secret keys must be destroyed after the session has ended.

The extra validation step for non-routine transactions is necessary because of the relative difficulty involved in securing personal computer applications on the Internet due to viruses, hackers, and individual ignorance. Banks should probably restrict routine money transfers available to ITT's to include only money transfers to well-known institutions, such as utility companies, major credit card vendors, and so on.

1.4.5. Terminal: Electronic Signature

1.4.5.1. Purpose

The electronic signature terminal (EST) is used by individuals to generate electronic signatures that cannot be forged for electronic documents. The EST either allows individuals to sign electronic documents, or verifies electronic signatures already on such documents.

1.4.5.2. Construction

The EST consists of:

- an BIA/PC
- a microcomputer
- a message digest encoder algorithm
- a modem, an X.25 connection, or an Internet connection
- an electronic signature software application

The EST uses an BIA/PC attached to a microcomputer, with events controlled by an electronic signature software application.

1.4.5.3. Identification

To create a digital signature without using some sort of public/private keyed token, three things need to be done. First, the document to be signed needs to be uniquely identified, the time of day needs to be recorded, and the individual performing the signature needs to be identified. This links the document, the individual, and the time, creating a unique time stamped electronic signature.

1.4.5.4. Operation

First the document to be signed is processed by a message digest encoding algorithm that generates a message digest code. One such algorithm is the MD5 algorithm by RSA, which is well known in the industry. By their nature, message digest algorithms are specifically designed so that it is almost impossible to come up with another document that generates the same message digest code.

Then, the individual enters his biometric-PIC using the BIA, the message digest code is handed to the BIA, the name of the document is added, and the resulting Digital Signature request message is sent to the DPC for authorization and storage.

When the DPC receives the request, it performs a biometric identity check, and once the individual is verified, it collects the message digest encoding, the individual's biometric account number, the current

time of day, the name of the document, and the identification of the BIA that gathered the signature, and stores them all in the Electronic Signatures Database (ESD). The DPC then constructs a signature code text string that consists of the ESD record number, the date, the time, and the name of the signer, and sends this signature code along with the individual's private code back to the EST.

To check an electronic signature, the document is sent through the MD5 algorithm (known in the industry), and the resulting value together with the electronic signature codes are given to the BIA along with the requesting individual's biometric-PIC, and the message is sent to the DPC. The DPC checks each signature for validity, and responds as appropriate.

1.4.5.5. Security

The BIA doesn't encrypt any of the data relating to electronic signatures, so document titles along with specific MD5 values are sent in plaintext. The same situation holds true for signature validations.

Thus while signatures cannot be forged, some of the details (including document names) are vulnerable to interception.

1.4.6. Terminal: Certified Email Terminal

1.4.6.1. Purpose

The purpose of the Certified Email Terminal (CET) is to provide individuals a way of delivering electronic messages to other individuals in the system while providing for identification of sender, verification of both receipt and recipient, and assuring confidentiality of message delivery.

The CET uses a BIA/PC to identify both the sender and the recipient. Security is established by encrypting the message, and then by encrypting the message key using the sender's BIA during the upload, and then decrypting the message key using the recipient's BIA during the download.

1.4.6.2. Construction

Both the transmitter and the recipient CET consists of:

- a BIA
- a microcomputer
- a modem, an X.25 connection, or an Internet connection
- the ability to receive email
- a certified electronic mail application

A CET is actually a microcomputer with an electronic mail application and a network connection which invokes the BIA to generate biometric-PIC authorizations to send and receive certified electronic mail.

1.4.6.3. Identification

In order to guarantee delivery of the message, both sender and recipients must be identified.

The sender identifies himself using his biometric-PIC when he uploads the message to the DPC. Each recipient the sender wishes to send the document to is identified either by biometric account identification number, or by fax number, and extension. In order for a recipient to download the message, he identifies himself using his biometric-PIC. This procedure resembles a person-to-person telephone call.

1.4.6.4. Operation

Message delivery starts with an individual uploading a document or message, and identifying himself using his biometric-PIC. The individual then verifies the name of the document, and the email message is encrypted and uploaded.

Once a message is uploaded, the sender receives a message identification code that can be used to request the current delivery status of the document to each of the recipients.

The DPC sends an electronic mail message to each recipient, notifying them when a certified message has arrived.

Once the recipient receives the notification, the recipient may at his leisure either choose to accept or refuse that message or a group of messages by submitting his biometric-PIC and having it validated by the DPC.

5 Once successfully transmitted to all recipients, a document is removed after a predetermined period, generally 24 hours. Individuals wishing to archive the document, along with an indication of all of the individuals to whom the message was sent may submit message archival requests prior to the deletion of the message.

10 1.4.6.5. Security

In order to effect the secure aspect of the transmission, the document is protected from disclosure en route. The CET accomplishes this using the 56-bit Message Key generated by the BIA. Since the BIA takes responsibility for encrypting the Message Key as part of the biometric-PIC, the encryption key is securely sent to the DPC.

15 When an individual downloads the message, the message key is sent encrypted along with the private code, to allow the recipient to decrypt the message. Note that it is fine to have all recipients have this message key, as they all receive the same message.

20 As with the ITT, individuals must take care to secure their CET application software from surreptitious modification, as a modified CET can send any document it wishes to once the individual validates the document name.

25 1.4.7. Terminal: Secure Fax Terminal

30 1.4.7.1. Purpose

The purpose of the secure fax terminal (SFT) is to provide individuals a way of delivering fax messages to other individuals in the system while providing for identification of sender, verification of both receipt and recipient, and assuring confidentiality of message delivery.

Each SFT uses an integrated BIA/catv to identify both the sender and the recipient. Communications security is accomplished through encryption.

1.4.7.2. Construction

Both the transmitter and the recipient SFT consists of:

- an BIA/catv
- a fax machine
- optional ISDN modem

A SFT is a fax machine connected to the DPC via a modem. The system treats faxes as just another type of certified electronic mail.

1.4.7.3. Identification

There are several different levels of security for secure faxes, but in the most secure version, the identity of the sender and all recipients is verified.

The sender identifies himself using his biometric-PIC and title index code when he sends his message to the DPC. To pick up the fax, each recipient listed identifies himself, again using biometric-PIC and title index code.

In addition, the receiving site is identified by phone number. This phone number is registered with the DPC. For secured- confidential faxes, each recipient is identified with the phone number and the extension.

1.4.7.4. Operation

There are five basic types of faxes that an SFT can send.

I. Unsecured Faxes

Unsecured faxes are equivalent to a standard fax. The sender enters the phone number of the recipient site, and sends the fax. In this case, the sender remains unidentified, and the fax is sent to a given phone

number in the hopes that it will be delivered to the proper recipient. An SFT marks the top line on all such unsecured faxes prominently as being "UNSECURED". All faxes received from non-SFT fax machines are always marked as being unsecured.

II. Sender-Secured Faxes

In a sender-secured fax, the sender selects the "sender-secured" mode on the fax machine, enters their biometric-PIC followed by their title index code. The fax machine then connects to the DPC, and sends the biometric-PIC information. Once the DPC verifies the individual's identity, the individual then sends the fax by feeding the document into the fax scanner. In this case, the fax is actually sent to the DPC, which stores the fax digitally. Once the entire fax arrives at the DPC, the DPC commences sending the fax to each destination, labeling each page with the name, title, and company of the sender, along with the banner of "SENDER-SECURED" at the top of each page.

III. Secured Fax

In a secured fax, the sender selects the "secured" mode on the fax machine, enters their biometric-PIC followed by their title index code, and then enters the phone numbers of the recipients. Once the system verifies the sender's identity and each of the recipients phone numbers, the individual then sends the fax by feeding the document into the fax scanner. The fax is then sent to the DPC, which stores the fax digitally. Once the entire fax arrives at the DPC, the DPC sends a small cover page to the destination indicating the pending secured fax, the sender's title and identity, as well as the number of pages waiting, along with a tracking code. This tracking code is automatically entered into the memory of the recipient's fax machine.

To retrieve the fax, any employee of the recipient company can select the "retrieve fax" button on his fax machine, select which pending fax to retrieve by using the tracking code, and then enter biometric-PIC. If the fax is unwanted, the individual may press the "reject fax" button, though he must still identify himself to the system in order to

do this. Once validated as a member of the company, the fax is then downloaded to the recipient's fax machine. Each page has "SECURED" on the top of each page, along with the sender's identity and title information.

IV. Secured Confidential Fax

In a secured-confidential fax, the sender selects the "secured-confidential" mode on the fax machine, enters his biometric-PIC followed by his title and index code, and then enters the phone number and system extension of each recipient. Once the DPC verifies the sender's identity and each of the recipients phone numbers and extensions, the individual then sends the fax by feeding the document into the fax scanner. The fax is sent to the DPC, which stores the fax digitally. Once the entire fax arrives at the DPC, the DPC sends a small cover page to each destination indicating the pending secured- confidential fax, the sender's title and identity, the recipient's title and identity, as well as the number of pages waiting, along with a tracking code. This tracking code is automatically entered into the memory of the recipient's fax. However, the only individual that can retrieve the fax is the individual whose extension code is indicated.

This individual selects the "retrieve fax" button, selects the pending fax to retrieve, and then enters his biometric-PIC. Once validated as the recipient, the fax is then downloaded to the recipient's fax machine. Each page has "SECURED-CONFIDENTIAL" on the top of each page, along with the sender's title and identity information.

V. Secured Confidential Contract Fax

This fax is processed identically to the secured- confidential fax in terms of the actual delivery of the fax to the recipients, except that the fax is titled "contract" instead of secured- confidential. In addition, the DPC automatically archives contract faxes. Any recipient may accept or reject the contract through the SFT subsequent to receiving the contract fax. Hence with the option, the DPC performs the role of an electronic notary.

5 Any fax that is sent to the system and then forwarded to the recipient may be sent to any number of recipients without tying up the sending fax machine. Additionally, the tracking number of any fax sent is entered into the memory of the fax machine; a status report on any ongoing fax can be generated at the sending machine by selecting the "status" button and then selecting the particular fax pending tracking code. The DPC issues a report that is immediately sent to the sending fax machine detailing the state of the sending for each recipient.

10 With any secured or secured-confidential fax, an option exists for either the sender or one of the recipients to archive the fax (along with the specifics as to who sent and received the fax) for future reference. To this end, any secured fax is retained for some time period (i.e., 24 hours) following successful delivery. An archival tracking code is returned to the individual whenever an archive is requested. This archival code is used to retrieve faxes and fax status reports archived with the system.

15 Archived faxes are placed on read-only secondary storage after some time period (i.e., 24 hours). Retrieving an archived fax requires human intervention, and may take up to 24 hours to perform.

20 1.4.7.5. Security

The SFT system works hard to assure the recipient of the sender's identity, and it works just as hard to assure the sender that the recipient actually acknowledged receipt of the document.

25 In order to protect against interception of the communications between the sender and recipient, the fax terminal encrypts the fax using the Message Key facility provided by the BIA. Since the BIA takes responsibility for encrypting the Message Key as part of the biometric-PIC, the encryption key is securely sent to the DPC.

30 When an individual receives a secured fax of any type, the message key is sent encrypted along with the private code, to allow the recipient to decrypt the message. Note that it is fine to have all recipients have this message key, as they all receive the same message.

1.4.7.6. Notes

Sending secured faxes is very similar to sending electronic mail, and reuses much of the same software.

It is possible to construct fax terminals that do not have integral BIA/fax devices but that have a port suitable for attaching an external BIA/pc and software appropriate for using the BIA.

1.4.8. Terminal: Biometric Registration Terminal

1.4.8.1. Purpose

The purpose of the Biometric Registration Terminal (BRT) is to register new individuals including their biometric-PIC, mailing address, private code, electronic mail addresses, a list of titles and title index codes used to send and receive electronic messages and faxes, and a list of financial asset accounts and account index codes that they can access, all using their biometric-PIC.

The objective of the enrollment process is to obtain personal information from an individual at the location of a responsible institution where that information can be validated. This includes, but is not limited to retail banking outlets, and corporate personnel departments. Each participating responsible institution has one BRT that is used by a group of employees who have been authorized to perform registrations. Each employee is accountable for each individual registered.

1.4.8.2. Construction

- an microcomputer and screen, keyboard, mouse
- an BIA/Reg
- 9.6 kb modem/X.25 network connection (known in the industry)
- a biometric registration software application

The BRT uses an attached BIA/Reg for biometric entry, and is connected to the system by a 9.6kb modem or an X.25 network connection

(known in the industry). Biometric registration terminals are located in places that are physically secure such as retail banking outlets.

1.4.8.3. Identification

5
Three entities need to be identified for the DPC to respond positively to an BIA/Reg registration request: the registering employee, the institution, and the BIA/Reg. The employee must have been authorized to register individuals for that institution.

10
The institution and the BIA are identified by cross-checking the owner of the BIA with the institution code set by the BRT. The employee identifies himself to the system by entering his biometric- PIC upon starting the registration application.

15
The institution uses its standard customer identification procedure (signature cards, employee records, personal information, etc) before registering the individual on the system. It is important for the institution to verify individual identity as assiduously as possible, since the registering individual will be empowered to transfer money from those accounts at will, and/or send electronic messages using the name of the
20
company.

1.4.8.4. Operation

25
During registration, the individual enters both a primary and secondary biometric. The individual must use both index fingers; if the individual is missing index fingers, the next inner-most finger may be used. Requiring specific fingers to be used allows the prior fraud check to work.

30
The individual is encouraged to select a primary and a secondary finger; the primary finger is given preference during the DPC identity check, so the individual should present the most-often used finger as the primary. Of course, the DPC could choose to alter the designation of primary and secondary biometrics based on operations if it turns out to be important to do so.

35
As a part of the biometric encoding process, the BIA/R determines if the individual has entered "a good print." Note that there are some individuals whose jobs result in the accidental removal of their

fingerprints, such as individuals who work with abrasives or acids. Unfortunately, these individuals cannot use the system. They are detected at this stage in the process and informed that they cannot participate.

5 The individual selects a PIC of from four to twelve digits from a series of PIC options provided by the system's central database. However, the PIC must be validated by the system. This involves two checks: one, that the number of other individuals using the same PIC aren't too great (since the PIC is used to reduce the number of individuals checked by the biometric comparison algorithm), and that the individual being registered isn't too "close", biometrically speaking, with other individuals within the same PIC group. If either happens, the enrollment is rejected, an error message is returned to the BRT, and the individual is instructed to request a different PIC. The system may optionally return with an "identical match" error condition, which indicates that the individual already has a record in the system under that PIC.

10 A PIC of 0 allows the system to assign a PIC to the individual.

The individual constructs a confidential private code consisting of a word or phrase. If the individual does not wish to construct one, a private code will be constructed randomly by the terminal.

20 The individual may also arrange their financial asset code list. This list describes which account index code points at which account (i.e. 1 for debit, 2 for credit, 3 for emergency debit, etc). Note that this can only occur if the registering institution is a bank, and only if the accounts are owned by that particular banking institution.

25 Even after registration, an individual is not actually able to perform operations using the system until a prior fraud check is completed. This generally takes a few minutes, but during times of high load, it takes up to several hours. Only if the system finds no instance of prior fraud is the individual's account activated.

30 1.4.8.5. Security

35 If an individual is found to have defrauded the system even once, the DPC institutes a database-wide involuntary biometric database search for the criminal. Several of these are performed each night, so individuals who are particularly wanted by the system are winnowed out of

the database by using a time consuming process during conditions of light activity.

5 The employees performing the registration operation identify themselves using biometric-PIC only when initially activating the registration system. This is a convenience for the employee, but a possible security problem for the system, as unattended or "temporarily borrowed" BRTs could be the source for fraud. As a result, the registration application exits after a predetermined period of no activity.

10 **1.4.9. Terminal: Customer Service**

1.4.9.1. Purpose

15 The purpose of the customer service terminal (CST) is to provide internal DPC support personnel access to the various aspects of the system databases. Support people need to answer inquiries by individuals, issuers, institutions, and merchants that are having trouble with the system.

20 **1.4.9.2. Construction**

The CST consists of:

- a microcomputer
- an BIA/Int
- 25 • ethernet/token ring/FDDI network interface
- a database examination and modification application

30 Each CST is connected to the system via a high speed local area network connection such as token ring, ethernet, fiber (FDDI), etc. Each CST has the capability to query each of the databases, and display the results of these queries. However, the CST only displays fields and records based on the privilege of the individual terminal user. For instance, a standard customer service employee won't be able to see the encryption code for a given BIA's VDB record, though they can see which merchant
35 or individual currently owns that BIA.

1.4.9.3. Identification

5 For the CST to allow access to the database, the individual and the BIA must be identified by the system. In addition, the individual's privilege level must also be determined, so that the database can restrict access appropriately.

1.4.9.4. Operation

10 An individual using a CST starts a session by providing identification by entering their biometric-PIC. The BIA constructs an Identification Request message, and send it to the DPC for verification. Once the system verifies the individual, the CST application can operate normally, though limited by the individual's previously assigned DPC
15 privilege level.

1.4.9.5. Security

20 For security purposes, the DPC will terminate a connection to the CST application after a predetermined idle time period.

It is important that the database application cannot be modified in any manner; either deliberately, or through an unintentional introduction of a virus. To that end, individual CSTs do not have any floppy drives or other removable media. Furthermore, read access to the database
25 application executable is strictly limited to those with a need to know.

In order to protect the communications between the CST and the database from surreptitious modification or disclosure, the CST encrypts all traffic between the CST and the database. To do this, the CST generates a session key that is sent to the server during the login session
30 with the system. This session key is used to encrypt and decrypt all communications with the DPC that occur during the period.

35 Even assuming secure communications and no modified database applications, the DPC makes certain that DPC data fields that are not accessible to the individual operating the CST are not sent to the CST's database application. Likewise, at no time do any CST personnel have access to or permission to modify individual biometric information.

The DPC and the support center can be co-located, or because of the fairly tight security surrounding the CST itself, the support center can be split off on its own.

5 **1.4.10. Terminal: Issuer Terminal**

1.4.10.1. Purpose

10 The purpose of the issuer terminal is to allow employees at issuing banks to submit batch asset account modification operations to the DPC in a secure and identifiable manner.

1.4.10.2. Construction

15 The IT consists of:

- a microcomputer
 - a modem, X.25 network, or Internet connection to the system
 - an BIA/Iss
 - a network connection to the bank's internal network
- 20

The Issuer Terminal uses an issuer BIA to authorize mass additions and deletions of financial asset information.

25 **1.4.10.3. Identification**

In this operation, the bank must be identified, a properly-authorized bank employee must be identified, and all of the individuals whose asset accounts are being added or removed must also be identified.

30 The bank is responsible for identifying the individuals who wish to add their accounts at that bank to their asset account list. As in biometric registration, this is done by the bank using signature cards and personal information. The DPC identifies the bank by cross-checking the issuer code submitted by the IT with the issuer code registered in the VAD record of the BIA/Iss. A biometric-PIC is used to identify the bank
35 employee actually submitting the batch.

1.4.10.4. Operation

5 In order to add a financial asset account, an individual gives his biometric identification number to the bank (the identification number is given to the individual during the initial biometric registration step) along with the accounts that are to be added. After the individual is properly identified, this identification code and account list are forwarded to the IT for subsequent batch submission to the system.

10 Whenever deemed appropriate by the bank, an authorized individual at the bank instructs the IT to upload the batched account additions/deletions to the DPC. To do this, the authorized individual enters his biometric-PIC, the IT adds a session key, adds the bank's issuer code, and from that the BIA/Iss constructs an Issuer Batch Request message that the IT then forwards to the DPC. The IT encrypts the batch using the message code, and then sends that as well.

15 When the system receives the Issuer Batch Request, it validates that the BIA is an BIA/Iss, that the BIA/Iss is registered to the bank claimed by the issuer code, and that the individual identified in the biometric-PIC is allowed to submit batch requests to the DPC for that bank. If so, the DPC processes all the requests, keeping track of errors as required. Once done, the DPC returns the individual's private code, along with an encrypted batch containing any errors that occurred during processing.

25 1.4.10.5. Security

30 Securing this transaction is critical for the security of the system. A criminal intent on fraud need only find a way to add other people's accounts to his biometric identification code and can then commit fraud at will. Eventually the criminal is caught, and purged from the database, but only after other people's accounts are drained by the criminal.

Encryption guarantees that the transmission between bank and DPC cannot be intercepted, and thus account numbers are protected in transit.

35 Cross-checking the bank with the BIA/Iss means that both the IT and the BIA must be compromised to submit false add/delete messages

to the DPC. Thus, the bank must ensure that the IT is physically secure, and that only authorized individuals are allowed to access it.

Requiring an individual to submit the batch provides for a responsible human to be "in the loop" whose job it is to make sure that proper bank security measures have been followed in the construction and submission of the batch.

1.4.11. Terminal: Automated Teller Machinery

1.4.11.1. Purpose

The purpose of the biometric ATM is to provide individuals access to cash and other ATM functions without having to use an Interbank card. It does this by submitting a biometric-PIC and an account index code and retrieving a bank account number. For users of the system, this replaces the Interbank card (known in the industry) + PIC mechanism as a method for identifying the account and authorizing the individual. It is assumed that all ATMs still continue to accept Interbank cards.

1.4.11.2. Construction

- a standard ATM
- an integrated BIA/ATM (scanner only)
- a connection to the DPC

The biometric ATM uses an integrated BIA/ATM to identify individuals and allow them access to financial assets using a biometric-PIC and an account index. An BIA/ATM is installed into the ATM, making use of the ATM's current PIC pad for PIC and account index code entry. The ATM is connected to the system using X.25 or modem.

The BIA/ATM is structured in such a way as to make integration with an existing ATM network as simple as possible. This results in a compromise between security and ease of integration.

1.4.11.3. Identification

5 Three entities need to be identified for the DPC to respond properly to an BIA/ATM account request: the individual, the bank, and the BIA/ATM.

10 The bank is identified by cross-checking the ATM's stored bank code with the BIA/ATM's bank code. The BIA/ATM is identified by successfully locating the BIA/ATM in the VAD, and the individual is identified through the standard biometric-PIC.

1.4.11.4. Operation

15 To access an ATM, an individual enters their biometric- PIC into the BIA along with the account index code. The BIA forms an account access request message, which is then sent to the DPC by the ATM. The DPC validates the biometric-PIC as well as the emergency account index code, and then sends the resulting asset account number along with the private code back to the ATM.

20 The ATM asks the BIA to decrypt the response, and then displays the private code on the ATM's display screen. The ATM also examines the response to see whether or not the individual is performing a standard account access, or a "duress" account access. If a duress account access is indicated, the ATM may provide false or misleading information as to the amounts available to the individual; the specifics of this behavior will vary from ATM to ATM. However, no ATM will ever provide any indication to the individual that a duress transaction is in progress.

1.4.11.5. Security

30 Messages between the ATM and the DPC are secured by encryption and MAC calculation from the BIA. The MAC means that the ATM cannot change the contents of the message without being detected, and encryption prevents the encrypted part of the message from being disclosed.

35 Because the BIA/ATM has no LCD or no PIC pad attached, it requires the ATM to provide all the text prompts and to gather all the input

from the individual. This is less secure than if the BIA were performing the operation, but as ATMs are generally physically robust, it can probably be called a wash.

5
1.4.11.6. Notes

10 It is between the bank and the individual to specify the behavior of an ATM when the individual indicates he is performing a transaction under duress. A particular bank may choose to limit access, or alter balance information, or a false screen may be displayed. A false screen is a display of data which has been intentionally pre-determined to be inaccurate such that a coercing party will not illegally obtain accurate data about an individual's financial assets. It is beyond the scope of the invention to specify the precise behavior of an ATM under these circumstances.

15
1.4.12. Terminal: Phone Point of Sale Terminal

1.4.12.1. Purpose

20 The purpose of the phone point of sale terminal (PPT) is to authorize credit or debit financial transactions from an individual using a specially-equipped telephone to make a purchase from a merchant.

25
1.4.12.2. Construction

The PPT consists of:

- an BIA/catv
 - a rapid-connect digital modem [see the VoiceView patent (known in the industry)]
 - a telephone (keypad, earpiece, microphone)
 - a microprocessor
 - a DSP (digital signal processor)
 - a standard telephone line
- 30

The PPT accepts biometric identification using an BIA/carv connected to and integrated with a cordless, cellular, or standard telephone.

1.4.12.3. Identification

In order for the DPC to authorize a transaction, both the individual and the merchant must be identified.

To identify an individual, biometric-PIC identification is used.

To identify a phone-order merchant, the merchant and all his phone numbers that individuals will call are registered with the DPC. Thus when an individual submits an authorization, he also submits the phone number he called, which is then cross-checked with the merchant's listed phone numbers.

1.4.12.4. Operation

Individuals call merchants that are selling their wares through paper catalogs, newspapers, magazines, or other basic print media mechanisms. The PPT uses a special modem that shares the telephone voice line to exchange digital information with the merchant.

Each time the individual makes a phone call, the PPT keeps track of the phone number that was typed by the user, in case the individual decides to make a purchase. A DSP is used to detect dialtone, ring, connection, and so on, in order to tell what the actual phone number entered was, as distinct from extensions, or the navigation of phone message systems, and so on.

Once a call is placed to a merchant, the salesman for the merchant digitally downloads all the relevant information to the PPT including product, price, and the merchant code. Note that when in operation, the modem disconnects the speaker.

When the product information is downloaded, the PPT then prompts the individual for the biometric-PIC, the account index code, and then asks the individual to validate the purchase amount. Then the phone number and the merchant code are added, and the message is encrypted.

The rapid-connect modem is again engaged to send the authorization information to the merchant.

When the merchant receives the authorization information, the merchant verifies that the price and product information are correct, and then forwards the transaction to the DPC using a secured communications channel using either the Internet or some other general purpose network. The connection to the DPC is secured using Public Key Encryption and a secret key exchange.

Upon receiving and decrypting a phone authorization, the DPC checks the phone number against the merchant code, validates the biometric-PIC, and then sends the transaction to the credit/debit network for authorization. If authorization succeeds, the DPC appends the buyer's address to the response message and sends the response to the merchant.

The merchant receives the response from the DPC, copies the mailing address, and forwards the message to the individual again via a brief session with the rapid-connect modem. When the transmission to the IPT is complete, a chime sounds, the modem disconnects, and the individual's private code (decrypted by the BIA) is displayed on the LCD screen. The merchant's sales rep confirms that the individual's mailing address is valid; if so, the call is terminated and the transaction is complete.

1.4.12.5. Security

One of the security concerns about phone transactions is the security of the phone system itself. Apart from the biometric identification, the central problem is making sure that the number the individual called actually reaches the merchant in question.

Note that the communications link between the PPT and the merchant isn't secured, so a purchase authorization from an individual to a merchant could be intercepted. However, no financial benefit would result from this, so it is not deemed to be important.

The security of a PPT is relatively low by necessity of price, weight, and because of the problems inherent in splitting the responsibility of PIC entry and private code decryption and presentation.

1.4.13. Terminal: Cable-TV Point of Sale

1.4.13.1. Purpose

5 The purpose of the CATV point of sale terminal (CPT) is to authorize credit or debit financial transactions from an individual in front of his television (or "TV") set to a merchant who is presenting objects for sale on television.

10 1.4.13.2. Construction

The CPT consists of:

- a BIA/catv
- a television remote control with integrated BIA/catv
- 15 • a Cable-TV digital signal decoder
- a Cable-TV remote control reader
- an on-screen display mechanism
- access to a Cable-TV broadband two-way communications channel

20 The CPT accepts biometric identification using an BIA/catv that is integrated with the television's remote control device. The remote control communicates with a television top box that itself communicates with the broadband cable television network. The terminal consists of the television remote logic that communicates with the BIA, as well as the television top box that communicates over the cable broadband network.

25 1.4.13.3. Identification

30 In this transaction, the merchant and the individual must both be identified to execute the transaction.

The individual is identified by the biometric-PIC.

35 The merchant is identified by a merchant credential, created by the CATV broadcaster at the time the product is shown on television. Each product broadcast has a merchant-product credential consisting of a merchant code, a time, a duration, and a price which is signed using Public

Key Encryption and the CATV network broadcaster's private key. This merchant-product credential can only be generated by the network broadcaster.

5 **1.4.13.4. Operation**

As a television advertisement, an infomercial, or a home shopping channel displays a product, the Cable television network also broadcasts simultaneous digital information that describes a short
10 description, price, as well as the merchant-product credential. This digital information is processed and temporarily stored by the CPT, ready to be accessed by the individual when a decision to purchase is made.

To buy something that is currently being displayed, the individual selects the on-screen display function of the special television
15 Remote, which instructs the CPT to display text information on the screen regarding the currently viewed product.

The individual is first prompted for the number of the items he wishes to buy through the on-screen display. Then he is prompted to enter his Biometric-PIC, and his account index code. Once he verifies that the
20 final purchase price is okay, the product, price, merchant code, merchant-product credential, and channel number along with the Biometric-PIC are used to construct a Remote Transaction Authorization request message. The request is sent to the merchant for authorization by way of the Cable-television broadband two-way communications channel.

25 Note that each merchant that desires to sell products in this manner must have the ability to receive order information using the broadband Cable television network.

Upon receipt of the authorization request, the merchant submits it to the DPC using a secured Internet connection or an X.25 connection.

30 If the DPC authorizes the transaction, it constructs an authorization response that includes the current mailing address of the individual in addition to the authorization code, and the encrypted private code. Once the merchant receives the authorization, he copies the authorization and the mailing address, and then forwards the authorization
35 back to the CPT, who then displays the private code to the individual, terminating the transaction.

1.4.13.5. Security

5 This architecture does not allow criminals to replay messages intercepted from the CableTV broadband, but they are able to read parts of them. If this is not desirable, then the messages may be encrypted using an optional CATV Center's public key, or other "link level" encryption between the CATV set-top box (known in the industry) and the CATV local office.

10 To secure a connection between a merchant and the DPC, the connection uses a session key changed daily that has been previously exchanged using a public key encryption key exchange system.

1.5. System Description: Data Processing Center

1.5.1. Introduction

15 The Data Processing Center (DPC) handles financial transaction authorizations and individual registration as its main responsibilities. In addition, the DPC provides storage and retrieval for secure faxes, electronic documents, and electronic signatures.

20 Each DPC site is made up of a number of computers and databases connected together over a LAN (known in the industry) as illustrated in the DPC Overview Figure (number**). Multiple identical DPC sites ensure reliable service in the face of disaster or serious hardware failure at any single DPC site. Furthermore, each DPC site has electrical power backup and multiple redundancy in all of its critical hardware and database systems.

25 DPC components fall into three categories: hardware, software, and databases. Below is a short description, by category, of each component. More detailed descriptions appear in the following sections.

1.5.1.1. Hardware

- FW Firewall Machine: the entry point of the DPC site.
- 5 GM Gateway Machine: the system coordinator and message processor.
- DPCLAN DPC Local Area Network: connects the DPC sites

1.5.1.2. Databases

- IBD Individual Biometric Database: identifies individuals from their biometric and PIC code.
- 15 PFD Prior Fraud Database: lists individuals who have defrauded the system and can check if a biometric matches any of these individuals.
- 20 VAD Valid Apparatus Database: stores information required to validate and decrypt BIA messages.
- AOD Apparatus Owner Database: stores information about the owners of BIA devices.
- 25 ID Issuer Database: identifies issuing banks that participate with the system.
- 30 AID Authorized Individual Database: stores the list of individuals allowed to use personal or issuer BIA devices.
- 35 RMD Remote Merchant Database: stores information necessary to process transactions with telephone and cable television merchants.

EDD Electronic Document Database: stores electronic documents, such as faxes and electronic mail, for retrieval by authorized individuals.

5 ESD Electronic Signature Database: stores electronic document signatures for verification by a third party.

1.5.1.3. Software

10 MPM Message Processing Module: handles the processing of each message by coordinating with the other software modules and databases required to perform the message's task.

15 SNM Sequence Number Module: handles DUKPT sequence number processing.

MACM Message Authentication Code Module: handles MAC validation and generation.

20 MDM Message Decrypt Module: handles encrypting and decrypting of BIA requests and responses.

25 PGL PIC Group List: handles the lookup of PIC groups by PIC and the configuration of database elements that depend on the list of PIC groups.

30 IML IBD Machine List: handles the lookup of the main and backup database machines dedicated to holding IBD records for a given PIC group.

1.5.1.4. Terminology

When defining database schema, the following terminology is used for describing field types:

int<X>	an integral type using <X> bytes of storage
char<X>	a character array of <X> bytes
text	a variable length character array
<type>[X]	a length <X> array of the specified type.
time	a type used for storing time and date
biometric	a binary data type used for storing the biometric
fax	a binary data type used for storing fax images

When describing database storage requirements, the term "expected" means the expected condition of a fully loaded system.

1.5.2. Protocol Description

Terminals accomplish their tasks by sending request packets to a DPC site. The DPC site sends back a reply packet containing the status on the success or failure of the request.

Communication is via a logical or a physical connection-oriented message delivery mechanism such as X.25 connections, TCP/IP connections, or a telephone call to a modem bank. Each session holds the connection to the terminal open until the DPC sends its response back to the terminal.

The request packet contains a BIA message part and a terminal message part:

- BIA message part
 - protocol version number
 - message type
 - 4-byte BIA Identification
 - 4-byte sequence number
 - <message specific data>
 - Message Authentication Code (MAC)

Terminal message part
 <terminal specific data>

5 The BIA message part is constructed by an BIA device. It includes one or two biometrics, a PIC, authorization amounts, and the contents of the general registers which are set by the terminal. Note: the MAC in the BIA message part only applies to the BIA part and not to the terminal part.

10 A terminal may place additional data for the request message in the terminal message part. The BIA provides a message key to allow the terminal to secure the terminal part data. The BIA automatically includes the message key in the packet's encrypted biometric-PIC block when necessary. The terminal performs the message key encryption itself, however.

15 The response packet contains a standard header and two optional free-form message parts: one with a MAC and one without:

Standard Header

protocol version number
 message type

Optional Free-form message part with MAC

<message specific data>
 MAC

Optional Free-form message part without MAC

<additional message specific data>

20
 25
 30 The message part with a MAC is sent to the BIA so that it may validate that this part of the response has not been tampered with and to display the individual's private code. The message part without a MAC is used for transmitting large amounts of data, such as fax images, that are not sent to the BIA for MAC validation as the BIA to terminal connection may be of limited bandwidth.

1.5.3. Processing Packets

5 In an embodiment of the invention with multiple DPC sites, a terminal need only send its request to one of the DPC sites, typically the closest, because that site automatically handles updating the others by running distributed transactions as necessary.

10 When one of the DPC's Firewall Machines receives a packet, it forwards it to one of the GM Machines for the actual processing. Each GM has a Message Processing Module that handles the coordination between the DPC components required to process the request and sends the response back to the sender.

1.5.4. Validating and Decrypting Packets

15 All packets the DPC receives, with the exception of those not constructed by an BIA, contain an BIA hardware identification code (the BIA Identification of the packet), a sequence number, and a Message Authentication Code (MAC). The GM asks the MAC Module to validate the packet's MAC and then checks the sequence number with the Sequence Number Module. If both check out, the GM passes the packet to the Message Decrypt Module for decryption. If any one of the checks fail, the GM logs a warning, terminates processing for the packet, and returns an error message to the BIA device.

20
25 Currently, the only message types that are not constructed by an BIA is the Secure Fax Data request and Electronic Document Data request.

1.5.5. Reply Packets

30 Each packet the DPC receives may contain an optional response key stored in the encrypted biometric-PIC block of the packet. Before the DPC replies to a request that includes a response key, it encrypts the reply packet with the response key. It also generates a Message Authentication Code and appends it to the packet.

35 The only exception to encrypting response packets applies to error messages. Errors are never encrypted and never include confidential

information. However, most response packets include a status or reply code that can indicate whether the request succeeded or not. For example, when the DPC declines a credit authorization, it does not return an error packet, it returns a normal transaction response packet with a reply code set to "failed".

1.5.6. DPC Procedures

The DPC has two procedures commonly used while processing requests.

1.5.6.1. Individual Identification Procedure

For requests that require the DPC to identify an individual, the DPC executes the following procedure: using the PIC code, the DPC searches the IBD Machine List for the main and backup IBD machines responsible for handling identifications for the given PIC code. Next, the DPC sends the identification request to either the main or backup machines depending on which is the least loaded. The IBD machine responds with the IBD record for the individual or an "individual not found" error.

The IBD machine retrieves all the IBD records for the given PIC. Using a proprietary biometric hardware device, the IBD machine compares each record's primary biometric with the individual's biometric arriving at a comparison score indicating the similarity of the two biometrics. If no biometric has a close enough comparison score, the comparisons are repeated using the secondary biometrics. If none of the secondary biometrics have a close enough comparison score, then the IBD machine returns an "individual not found" error. Otherwise, the IBD machine returns the full IBD record of the individual, from which such fields such as the private code, account numbers, titles, and so on may be obtained.

1.5.6.2. Emergency Response Procedure

For requests that include an account index, the DPC handles the case where the individual chooses his or her emergency account index. The

GM processing the request immediately notifies the DPC customer support staff, logs a warning, and if the response packet has a reply code, sets it to "emergency". It is the responsibility of the owner of the BIA device that submitted the request to watch for an "emergency" reply code and provide further assistance, such as the false screen mechanism described in the ATM terminal section. The DPC also increments the emergency use count of the individual's IBD record whenever the emergency account index gets accessed.

1.5.7. Protocol Requests

The following sections describe each protocol request/response and the actions the DPC takes to perform them.

The list of protocol packets are:

- Individual Identification
- Transaction Authorization
- Registration
- Account Access
- Issuer Batch
- Secure Fax Submit
- Secure Fax Data
- Secure Fax Tracking
- Secure Fax Retrieve
- Secure Fax Reject
- Secure Fax Archive
- Secure Fax Contract Accept
- Secure Fax Contract Reject
- Secure Fax Organization Change
- Electronic Document Submit
- Electronic Document Data
- Electronic Document Tracking
- Electronic Document Retrieve
- Electronic Document Reject
- Electronic Document Archive

- Electronic Document Archive Retrieve
- Electronic Signature
- Electronic Signature Verify
- Network Credential

5

1.5.7.1. Individual Identification

Individual Identification Request

BIA Part:

10

4-byte BIA Identification

4-byte sequence number

encrypted(DUKPT key) Biometric-PIC block:

300-byte authorization biometric

4-12 digit PIC

15

56-bit response key

MAC

Terminal Part: (not used)

Individual Identification Response

20

encrypted(response key):

private code text

individual name

biometric identification code

MAC

25

The Individual Identification request includes a biometric-PIC block which the DPC uses with the individual identification procedure to identify the individual. If the individual is identified, then the DPC responds with the individual's name, biometric identification, and private code. Otherwise, the DPC responds with an "unknown individual" error.

30

1.5.7.2. Transaction Authorization

Transaction Authorization Request

BIA Part:

- 5 4-byte BIA Identification
- 4-byte sequence number
- encrypted(DUKPT key) Biometric-PIC block:*
- 300-byte authorization biometric
- 4-12 digit PIC
- 10 56-bit response key
- [optional 56-bit message key]
- account index
- price
- merchant Identification
- 15 [optional free-format product information]
- [optional merchant code (phone#, channel# + time, hostname)]
- [optional send-address request]
- MAC

Terminal Part: (not used)

20

Transaction Authorization Response

encrypted(response key):

- private code text
- authorization response
- 25 authorization detail (autho code, transaction identification, etc)
- [optional individual address information]
- reply code (fail, ok, emergency)
- MAC

30

There are two basic transaction authorization subtypes: retail and remote.

For retail authorizations, the DPC identifies the purchasing individual by the biometric-PIC block of the request. If the individual cannot be identified, the DPC replies with an "unknown individual" error.

35

Next, the DPC sends an external authorization request (crediting the asset account of the BIA device's owner and debiting the

individual's asset account) to one of several existing financial authorization services depending on the type of asset accounts involved (such as Visa™ or American Express™). If the external financial authorization service approves the transaction, the DPC returns the external authorization codes and an "ok" reply code to the BIA device. Otherwise, the DPC returns the reason why the authorization was denied and sets the reply code to "failed". In either case, the DPC includes the individual's private code in the response.

When the DPC looks up the individual's asset account using the account index of the request, the chosen account may be the "emergency" account. If this happens, the DPC follows the emergency response procedure. The external authorization still takes place, however.

Remote authorization are generated by telephone, mail-order, or cable television merchants. The DPC handles remote authorizations the same way it does a retail authorization but with the following exceptions:

i) Remote authorizations include a remote merchant code which the DPC checks against the Remote Merchant Database to validate whether the packet's merchant Identification matches the one stored in the database. Furthermore, the asset account credited is the remote merchant's account, not the account of the BIA device's owner.

ii) Additionally, BIA devices that generate the remote authorizations tend to be personal BIA devices. The DPC checks the biometric Identification of the identified individual against the Authorized Individual Database's list of individuals allowed to use the BIA device. If the individual is not authorized to use the device, then the DPC denies the authorization request.

iii) Finally, the authorization packet may contain a "send-address" indicator. This indicator informs the DPC to include the individual's address in the reply packet and is usually used only for mail order purchases.

1.5.7.3. Registration

Registration Request

BIA Part:

- 4-byte BIA Identification
- 4-byte sequence number

encrypted(DUKPT key) Biometric-PIC block:

1000-byte primary biometric
 1000-byte secondary biometric
 4-12 digit PIC

5 56-bit response key
 56-bit message key
 MAC

Terminal Part:

encrypted(message key):

10 name
 address
 zipcode
 private code
 15 asset account list (account index code, account #)
 emergency account (account index code, account #)
 title list (title index code, title name)

Registration Response

status code

20 *encrypted(response key):*

private code text
 PIC
 biometric Identification code
 list of DPC chosen PICs (if original choice of PIC
 25 is rejected)

status code (ok, rejected)

MAC

30 Individuals register with the DPC via a Biometric Registration
 Terminal (BRT). The BRT sends the DPC a registration packet containing
 primary and secondary biometrics and personal identification code, along
 with ancillary data such as the individual's name, address, a list of financial
 asset accounts, the private code, and the emergency account. Optionally,
 the individual may include an electronic mail address, and a title list
 35 including titles and the title index code, as well as an Social Security
 Number (or "SSN"). The individual may choose his or her own PIC code

or allow the system to choose it. In a modification step any previously entered data can be modified or deleted.

At any given moment, only one DPC site acts as the registration site, for implementation simplicity. Registration request packets received by non-registration DPC sites are forwarded to the current registration site. The registration DPC site performs the entire registration check, assigning of IBD records to IBD machines, and the distributed transaction required to update all other DPC sites.

The registration DPC site selects the PIC code for registration requests that don't specify one, stores the IBD record on the main and backup IBD machines (as specified in the PIC Group List), and checks the PIC and biometric suitability of the registration packet before running the distributed transaction to update the other DPC sites.

The DPC runs a personal identification code and biometric sample duplication check step wherein the biometrics and personal identification code gathered during the registration step is checked against all previously registered biometrics currently associated with the identical personal identification code. The DPC may reject the registration for the following reasons: the PIC code is too popular, or the biometrics are too similar to other biometrics stored under the chosen PIC. To aid the individual in choosing an acceptable PIC, the DPC generates a short list of PIC codes for which the registration will be guaranteed that it reserves for a period of time. The BRT then prompts the individual for a new PIC which may be chosen from the good PIC list.

1.5.7.4. Account Access

Account Access Request

BIA Part:

4-byte BIA Identification

4-byte sequence number

encrypted(DUKPT key) Biometric-PIC block:

300-byte authorization biometric

4-12 digit PIC

56-bit response key

[optional 56-bit message key]

account index

MAC

Terminal Part: (not used)

5

Account Access Response

encrypted(response key):

private code text

[optional PIC]

asset account number

10

reply code (fail, ok, emergency)

MAC

The account access request allows BIA-equipped Automated Teller Machines to provide a safer and more convenient way for individuals to identify themselves to the ATM.

15

The GM identifies the individual by the packet's biometric-PIC and uses the specified account index to choose which asset account number to retrieve.

When the GM looks up the individual's asset account using the account index of the request, the chosen account may be the "emergency" account. If this happens, the GM follows the emergency response procedure.

20

1.5.7.5. Issuer Batch

25

Issuer Batch Request

BIA Part:

4-byte BIA Identification

4-byte sequence number

30

encrypted(DUKPT key) Biometric-PIC block:

300-byte authorization biometric

4-12 digit PIC

56-bit response key

56-bit message key

35

issuer code

MAC

*Terminal Part:**encrypted(message key) batch list:*

add <biometric Id> <account index> <asset account> [<emergency flag>]
 remove <biometric Id> <account index> <asset account>

Issuer Batch Response*encrypted(response key):*

private code text

reply code (fail, ok, emergency)

MAC

encrypted(message key) failed list:

failed <command> <code>

...

The Issuer Batch request allows an issuing bank or other authority to perform routine maintenance on the Individual Biometric Database. The DPC logs a security violation warning if it receives any Issuer Batch requests from non-issuer BIA devices, and it also refuses to process the request.

The DPC identifies the individual submitting the batch request by following the individual identification procedure. The DPC then checks that the individual is registered in the Authorized Individual Database to use the BIA device embedded in the sending Issuer Terminal.

The DPC also uses the issuer code in the request to look up the apparatus owner Identification in the Issuer Database and compare it against the apparatus owner Identification stored in the Valid Apparatus Database to ensure that the issuer code is not forged.

The DPC then executes the add and delete commands in the message-key encrypted batch list. The batch list is a newline separated list of commands. Valid commands are:

add <biometric Id> <account index> <asset account> [<emergency flag>]
 remove <biometric Id> <account index> <asset account>

The add command adds the asset account to the account list at the specified account index. The optional emergency flag indicates whether the particular account index is treated as the individual's emergency account. If the

asset account currently stored in the account list does not belong to the issuer, the command fails. This feature prevents one bank from adding or removing asset accounts from other bank's customers without the individual's knowledge or authorization.

5 The remove command clears the individual's asset account stored at the specified account index in the account list. If the asset account currently stored in the account list does not match the account the issuer is attempting to remove, the command fails.

10 For each command in the batch that failed to execute correctly, the GM logs a security violation warning and appends an entry to the failed list of the response. The failed entry includes the text for the command and the error code.

15 **1.5.7.6. Secure Fax Submit**

Secure Fax Submit Request

BIA Part:

4-byte BIA Identification

4-byte sequence number

20 *encrypted(DUKPT key) Biometric-PIC block:*

300-byte authorization biometric

4-12 digit PIC

56-bit response key

56-bit message key

25 security mode (unsecured, sender-secured, secured, secured-confidential)

sender title index code

sender fax number

sender fax extension

recipient list

30 [optional archive fax indicator]

[optional contract/agreement indicator]

Terminal Part: (not used)

Secure Fax Submit Response

encrypted(response key):
private code text
fax tracking number
MAC

5

When the DPC receives a Secure Fax Submit request, it identifies the individual from the request's biometric-PIC by following the individual identification procedure. This identification, along with the individual's title described by the title index code, is presented to the recipients so that the sender of the fax is always reliably identified.

10

The DPC generates a tracking number for tracking purposes and stores it, the sender's biometric Identification, the security mode, and the message key in a newly created EDD Document record. For each recipient in the recipient list, the DPC also creates a Recipient record. The DPC then waits for the sending fax machine to transmit the fax data encrypted under the message key.

15

If the request includes an "archive fax" or "contract/agreement" indicator, the EDD places a copy of the Document and Recipient records in the archive database. Any subsequent updates to these records are also made to the archived versions.

20

The fax data is sent in a separate step so that if the sender makes a mistake entering his biometric and PIC, the system notifies him before he wastes any time feeding the document into the fax machine.

25

1.5.7.7. Secure Fax Data

Secure Fax Data Request

BIA Part: (not used)

Terminal Part:

fax tracking number
encrypted(message key):
fax image data

30

Secure Fax Data Response

status (incomplete, ok)

35

The Secure Fax Data request allows a secure fax machine to send the fax image to the DPC for delivery to the previously specified recipient(s). This request does not involve any biometric identification and instead relies upon the secret message key to securely transmit the image.

5

The fax image data is encrypted by the message key registered by the Secure Fax Submit request. Once the DPC has received the entire fax, it sends a Secure Fax Arrival Notice message to each of the recipient's fax numbers. The DPC retrieves the list of recipients by querying the EDD for all Recipient records containing the fax tracking number. The Recipient record contains the destination fax number and optional extension. After sending the Arrival Notice, the DPC updates each Recipient record's delivery status field to "notified". Note: if the destination fax number is busy, the DPC marks the delivery status field to "busy" and retries sending the notice periodically (i.e., every 10 minutes) until successful and at that time, updates the status field to "notified".

10

15

The Arrival Notice is as follows:

Secure Fax Arrival Notice (Fax message)

- sender name, company, title, and fax number
- fax tracking number
- instructions on how to download the fax

20

The DPC only sends the sender a Status Notice via fax after all recipients have either retrieved or rejected the fax. The sender may query the DPC using the Secure Fax Tracking request (see below) to get the current status of all recipients.

25

The Status Notice is as follows:

Secure Fax Status Notice (Fax message)

- sender name, company, title, and fax number
- fax tracking number
- list of recipients showing:
 - name, company, title, and fax number
 - delivery date and status
 - contract/agreement status

30

35

The DPC finds each individual's company and title information in the EDD Organization table.

For individuals who are not registered in the system and hence cannot receive secure faxes or for non-recipient secured modes, the DPC does not send them a Secure Fax Arrival Notice. Instead, the DPC sends them the fax directly. If the fax line is busy, the DPC retries every 10 minutes until it succeeds in delivering the fax.

1.5.7.8. Secure Fax Tracking

Secure Fax Tracking Request

BIA Part:

4-byte BIA Identification

4-byte sequence number

encrypted(DUKPT key) Biometric-PIC block:

300-byte authorization biometric

4-12 digit PIC

56-bit response key

56-bit message key

fax tracking number

MAC

Terminal Part: (not used)

Secure Fax Tracking Response

encrypted(response key):

private code text

message digest for tracking response fax image

status code (ok, failed)

MAC

fax image for recipient status list

The DPC handles the Secure Fax Tracking request by retrieving all EDD Recipient records for the fax and generating a fax message to display the records. If the individual making the tracking request is not the sender of the fax document, then the DPC sets the status code to failed and puts an empty fax in the response.

The tracking response fax contains information describing the status of the delivery of the fax to each recipient. This fax contains such status information as line busy, fax arrival notice sent, fax sent, fax rejected, contract accepted, and so on.

5

The Tracking Notice is as follows:

Secure Fax Tracking Notice (Fax message)

sender name, company, title, and fax number

fax tracking number

10

list of recipients showing:

name, company, title, and fax number

delivery date and status

contract status

15

1.5.7.9. Secure Fax Retrieve

Secure Fax Retrieve Request

BIA Part:

4-byte BIA Identification

20

4-byte sequence number

encrypted(DUKPT key) Biometric-PIC block:

300-byte authorization biometric

4-12 digit PIC

56-bit response key

25

fax tracking number

MAC

Terminal Part: (not used)

Secure Fax Retrieve Response

30

encrypted(response key):

private code

56-bit message key

status (incomplete, ok, invalid recipient)

message digest for fax image

35

MAC

encrypted(message key):

fax image

5 The DPC uses the biometric-PIC to identify the individual making the retrieve request by following the individual identification procedure. If no EDD Recipient record exists for the individual and for the specified fax, then the DPC responds with an "invalid recipient" status.

The DPC retrieves the encrypted fax image from the EDD Document record with the correct fax tracking number and biometric Identification which it returns to the requester.

10 The fax image includes a cover page that displays whether the fax is a contract/agreement and the sender's name, company, title, fax number, and extension.

15 When the last recipient has either received or rejected the fax, the DPC sends a Status Notice via fax (see Secure Fax Data, above) to the fax's sender and then schedules to remove the Document and Recipient records from the EDD within a configurable time period. The time period is intended to allow the recipients sufficient time to decide whether or not to archive the fax.

20 1.5.7.10. Secure Fax Reject

Secure Fax Reject Request

BIA Part:

25 4-byte BIA Identification

4-byte sequence number

encrypted(DUKPT key) Biometric-PIC block:

300-byte authorization biometric

4-12 digit PIC

56-bit response key

30 fax tracking number

MAC

Terminal Part: (not used)

Secure Fax Reject Response

35 *encrypted(response key):*

private code

status code (ok, invalid recipient)
MAC

5

The DPC uses the biometric-PIC to identify the individual making the secure fax reject request. The DPC finds the EDD Recipient record keyed by the request's fax tracking number and the individual's biometric Identification. If the record cannot be found then the request fails with an "invalid recipient" status.

10

When the last recipient has either received or rejected the fax, the DPC sends a Status Notice via fax (see Secure Fax Data, above) to the fax's sender and then schedules to remove the Fax and Tracking records from the EDD within a configurable time period. The time period is intended to allow the recipients sufficient time to decide whether or not to archive the fax.

15

1.5.7.11. Secure Fax Archive

Secure Fax Archive Request

BIA Part:

20

- 4-byte BIA Identification
- 4-byte sequence number
- encrypted(DUKPT key) Biometric-PIC block:*
 - 300-byte authorization biometric
 - 4-12 digit PIC
 - 56-bit response key
- fax tracking number
- MAC

25

Terminal Part: (not used)

Secure Fax Archive Response

30

- encrypted(response key):*
 - private code
 - status code (ok, invalid individual)
 - MAC

35

The DPC uses the biometric-PIC to identify the individual making the secure fax archive request. The DPC finds the EDD Recipient record keyed

by the request's fax tracking number and the individual's biometric Identification. If the record cannot be found and the individual is not the sender or one of the recipients, then the request fails with an "invalid individual" status. Otherwise, the DPC copies the Document and Recipient records into the EDD archive database. Any subsequent changes to these records are also copied to the archived versions.

1.5.7.12. Secure Fax Contract Accept

Secure Fax Contract Accept Request

BIA Part:

4-byte BIA Identification

4-byte sequence number

encrypted(DUKPT key) Biometric-PIC block:

300-byte authorization biometric

4-12 digit PIC

56-bit response key

fax tracking number

MAC

Terminal Part: (not used)

Secure Fax Contract Accept Response

encrypted(response key):

private code

status code (ok, invalid recipient)

MAC

The DPC uses the biometric-PIC to identify the individual making the Contract Accept request. The DPC finds the EDD Recipient record keyed by the request's fax tracking number and the individual's biometric Identification. If the record cannot be found then the request fails with an "invalid recipient" status. Otherwise, the DPC updates the Recipient record's contract status field to "accepted" and generates a Status Notice to the fax's sender (see Fax Data, above).

1.5.7.13. Secure Fax Contract Reject

Secure Fax Contract Reject Request

BIA Part:

5 4-byte BIA Identification
 4-byte sequence number
 encrypted(DUKPT key) Biometric-PIC block:
 300-byte authorization biometric
 4-12 digit PIC
 10 56-bit response key
 fax tracking number
 MAC

Terminal Part: (not used)

15 Secure Fax Contract Reject Response

encrypted(response key):
 private code
 status code (ok, invalid individual)
 MAC

20 The DPC uses the biometric-PIC to identify the individual making
 the Contract Reject request. The DPC finds the EDD Recipient record keyed
 by the request's fax tracking number and the individual's biometric
 Identification. If the record cannot be found then the request fails with an
 25 "invalid recipient" status. Otherwise, the DPC updates the Recipient record's
 contract status field to "rejected" and generates a Status Notice to the fax's
 sender (see Fax Data, above).

30 1.5.7.14. Secure Fax Organization Change

Secure Fax Organization Change (Secure Fax message)
 sender name, company, title, and fax number
 list of organizational changes

35 Organization changes are submitted to the DPC via a secure fax
 message. A customer support engineer enters the changes requested in the fax

message, verifying that the individual submitting the request is allowed to register individuals for that particular company. Since the fax is a secure fax, the sender's identity has already been ascertained, as has his title.

5 **1.5.7.15. Electronic Document Submit**

Electronic Document Submit Request

BIA Part:

4-byte BIA Identification

4-byte sequence number

encrypted(DUKPT key) Biometric-PIC block:

300-byte authorization biometric

4-12 digit PIC

56-bit response key

56-bit message key

recipient list

MAC

Terminal Part: (not used)

20 **Electronic Document Submit Response**

encrypted(response key):

private code text

tracking number

status code (ok, invalid recipient)

MAC

When the DPC receives an Electronic Document Submit request, it identifies the individual by following the individual identification procedure.

30 The DPC then creates an EDD Document record and assigns it a unique tracking number. The DPC initializes the record's sender identification code to be the biometric identification code of the identified individual and the message key to be the message key in the request.

35 Next, the DPC searches the Individual Biometric Database for each recipient and creates an EDD Recipient record for each one. Each record is initialized with the tracking number, the recipient's biometric identification

code, and a delivery status of "incomplete". If any of the recipients cannot be found, the DPC replies with an "invalid recipient" status.

1.5.7.16. Electronic Document Data

5

Electronic Document Data Request

BIA Part: (not used)

Terminal Part:

tracking number

10

command (either abort or data)

[optional message offset]

completion indication

encrypted(message key):

message body

15

Electronic Document Data Response

status (incomplete, ok)

The Electronic Document Data request allows an individual to send the document text (in one or more parts) to the EDD for delivery to the recipient(s). This request does not involve any biometric identification, instead, it relies upon the secret message key to securely transmit the document text.

20

The request text is assumed to be encrypted by the message key stored in the EDD document record and is appended to the document text already stored in the record.

25

When the EDD receives a packet with the "document complete" indicator, it knows that the sender has finished transmitting the document. The EDD now sends an Arrival Notice to all recipients of the document via Internet electronic mail informing them that they have a document waiting.

30

The Arrival Notice is as follows:

Electronic Document Arrival Notice (Internet E-mail message)

sender name, company, title, and e-mail address

tracking number

35

instructions on how to receive the electronic document

The EDD also updates the status of the EDD recipient record to "notified". When all recipients have either retrieved or rejected the electronic document, the DPC sends a Status Notice via Internet electronic mail to the document originator.

5

The Status Notice is as follows:

Electronic Document Status Notice (Internet E-mail message)

sender name, company, title, and e-mail address

tracking number

10

list of recipients showing for each

name, company, title, e-mail address

delivery date and status

15

The DPC finds each individual's company and title information in the EDD Organization table.

1.5.7.17. Electronic Document Retrieve

Electronic Document Retrieve Request

20

BIA Part:

4-byte BIA Identification

4-byte sequence number

encrypted(DUKPT key) Biometric-PIC block:

25

300-byte authorization biometric

4-12 digit PIC

56-bit response key

tracking number

MAC

30

Terminal Part: (not used)

Electronic Document Retrieve Response*encrypted(response key):*

private code

56-bit message key

status (incomplete, ok, invalid recipient)

MAC

encrypted(message key):

document text

The DPC uses the biometric-PIC to identify the individual making the electronic document retrieve request by following the individual identification procedure.

The DPC next finds the EDD Recipient record keyed by the tracking number and the individual's biometric Identification.

If the record cannot be found, then the request fails with an "invalid recipient" status. Otherwise, the DPC sends the document's message key and the document (still encrypted by the message key) to the requester.

The EDD then updates the status of the EDD recipient record to "retrieved". When all recipients have either retrieved or rejected the document, the DPC sends a Status Notice via Internet electronic mail to the document originator (see Electronic Document Data, above) and then schedules to remove the Document and Recipient records (see Secure Fax Retrieve, above).

1.5.7.18. Electronic Document Reject**Electronic Document Reject Request***BIA Part:*

4-byte BIA Identification

4-byte sequence number

encrypted(DUKPT key) Biometric-PIC block:

300-byte authorization biometric

4-12 digit PIC

56-bit response key

message tracking number

MAC

Terminal Part: (not used)

Electronic Document Reject Response

encrypted(response key):

private code

status code (ok, invalid recipient)

MAC

The DPC uses the biometric-PIC to identify the individual making the electronic document reject request. The DPC next finds the EDD Recipient record keyed by the tracking number and the individual's biometric Identification. If the record cannot be found, then the request fails with an "invalid recipient" status.

The EDD updates the status of the EDD recipient record to "rejected". The DPC then follows the same notification and deletion procedure as described in Electronic Document Retrieve, above.

1.5.7.19. Electronic Document Archive

Electronic Document Archive Request

BIA Part:

4-byte BIA Identification

4-byte sequence number

encrypted(DUKPT key) Biometric-PIC block:

300-byte authorization biometric

4-12 digit PIC

56-bit response key

tracking number

MAC

Terminal Part: (not used)

Electronic Document Archive Response

encrypted(response key):

private code

status code (ok, invalid individual)

MAC

The DPC uses the biometric-PIC to identify the individual making the electronic document archive request. The DPC finds the EDD Recipient record keyed by the request's tracking number and the individual's biometric Identification. If the record cannot be found and the individual is not the sender or one of the recipients, then the request fails with an "invalid individual" status. Otherwise, the DPC copies the Document and Recipient records into the EDD archive database. Any subsequent changes to these records are also copied to the archived versions.

1.5.7.20. Electronic Document Archive Retrieve

Electronic Document Archive Retrieve Request

BIA Part:

4-byte BIA Identification

4-byte sequence number

encrypted(DUKPT key) Biometric-PIC block:

300-byte authorization biometric

4-12 digit PIC

56-bit response key

optional title index code, sending fax number, and extension tracking number

MAC

Terminal Part: (not used)

Electronic Document Archive Retrieve Response

encrypted(response key):

private code

status code (ok, invalid individual)

MAC

The DPC can receive an Electronic Document Archive Retrieve request from either a Secure Fax Terminal or a Certified Email Terminal. The DPC uses the individual identification procedure to determine the individual submitting the archive retrieve request. The individual must be either the sender or one of the recipients or else the DPC denies the request by setting the status code to "invalid individual". However, if the archived document was

a fax sent using a corporate title, the DPC allows additional individuals whose titles are higher in the corporate hierarchy to retrieve the archived document as well.

5 The EDD maintains an archive database, indexed by the document's original tracking number, stored on off-line media such as CD-ROMs and tape that can take considerable time to search for the archived document. As a result, the DPC does not return the archived document immediately, but instead informs the requesting individual that the DPC has begun the search. At
10 a later date when the DPC finishes the search, it notifies the requester that the archived document is ready to be retrieved through the standard document arrival notification mechanisms -- either via fax or email, depending on the format of the original document.

15 The DPC creates an EDD archive request record to store information about the requester so that when the search completes, the DPC remembers to whom to send the document.

1.5.7.21. Electronic Signature

Electronic Signature Request

BIA Part:

4-byte BIA Identification

4-byte sequence number

encrypted(DUKPT key) Biometric-PIC block:

300-byte authorization biometric

4-12 digit PIC

56-bit response key

document name

document MD5 calculation

MAC

30 *Terminal Part: (not used)*

Electronic Signature Response

encrypted(response key):

private code text

signature string

MAC

To process the electronic signature request, the DPC first performs a biometric identification using the biometric-PIC. Then, the DPC creates an ESD record, assigns it a unique signature identification code, and sets the record's signature field to the electronic signature in the request. The DPC then returns a signature string that can be submitted for later verification:

"<Dr. Bunsen Honeydew> <Explosions in the Laboratory> 5/17/95 13:00
PST 950517000102"

1.5.7.22. Electronic Signature Verify

Electronic Signature Verification Request

BIA Part:

4-byte BIA Identification

4-byte sequence number

encrypted(DUKPT key) Biometric-PIC block:

300-byte authorization biometric

4-12 digit PIC

56-bit response key

signature string

MAC

Terminal Part: (not used)

Electronic Signature Verification Response

encrypted(response key):

private code text

signature string

status (verified, failed)

MAC

The DPC performs a biometric identification, extracts the signature tracking code from the signature string, retrieves the indicated ESD record, and verifies that it matches the signature string. The DPC returns the private code and the outcome of the signature comparison.

1.5.7.23 Network Credential

Network Credential Request

BIA Part:

5 4-byte BIA Identification
 4-byte sequence number
 encrypted(DUKPT key) Biometric-PIC block:
 300-byte authorization biometric
 10 4-12 digit PIC
 56-bit response key
 account index
 bank code
 bank hostname
 terminal.port and bank.port (TCP/IP addresses)
 15 MAC

Network Credential Response

encrypted(response key):
 private code
 20 *signed(DPC's private key):*
 credential(time, acct, terminal.port, bank.port)
 bank's public key
 status code (ok, failed)
 25 MAC

30 The DPC identifies the individual using the request's biometric-PIC and retrieves the individual's asset account stored at the specified index. If the account index is the emergency account, then the network credential response status code is set to "failed" and no credential is generated.

 The DPC constructs the credential using the current time, the retrieved asset account, and the TCP/IP addresses of the terminal and the bank. The DPC then uses public key encryption to sign the credential with its private key.

35 The response also includes the bank's public key, which the DPC retrieves from the Remote Merchant Database.

1.5.8. Customer Support and System Administration Messages

5 The DPC handles additional message types classified as internal messages. The DPC generally does not accept these messages from non-DPC systems. The messages are database vendor specific. However, the internal network uses DES-encrypted packets to provide additional security.

The Customer Service and System Administration tasks are implemented using the database vendor's query language and application development tools.

1.5.8.1. Customer Service tasks:

- IBD: find, activate, deactivate, remove, correct records.
- AID: add or remove authorized individuals.
- 15 • AOD: find, add, remove, correct records.
- VAD: find, activate, deactivate, remove, correct records.
- RMD: find, add, remove, correct records.
- PFD: add, remove, correct records.

1.5.8.2. System Administration tasks:

- Run prior fraud checks.
- Modify the Valid Site List.
- Summarize log information (warnings, errors, etc.).
- 25 • Modify the PIC Group List.
- Performance monitoring.
- Run backups.
- Crash recovery procedures.
- Time synchronization for the DPC sites.
- 30 • Change the primary registration site.
- Change the secret DES encryption key.
- Clean up old document tracking numbers.
- Generate a list of BIA hardware identification code, MAC encryption key, and DUKPT Base Key triples. Store on an encrypted floppy
35 for the Key Loading Device.

1.5.9. Firewall Machine

1.5.9.1. Purpose

5 The FW Machines provide a first line of defense against network viruses and computer hackers. All communication links into or out of the DPC site first pass through a secure FW Machine.

1.5.9.2. Usage

10 The FW Machine, an internet-localnet router, only handles messages destined for the GM Machines.

15 BIA-equipped terminals send packets to a single DPC site via modem, X.25, or other communication medium. The DPC relies on a third party to supply the modem banks required to handle the volume of calls and feed the data onto the DPC backbone.

20 For DPC to DPC communication, primarily for distributed transactions and sequence number updates, the FW Machines send out double-length DES encrypted packets. The DPC LAN component handles the encryption and decryption: the FWs do not have the ability to decrypt the packets.

1.5.9.3. Security

25 A properly configured network sniffer acts as an intruder detector as backup for the FW. If an anomalous message is detected, the intruding messages are recorded in their entirety, an operator is alerted, and the FW is physically shut down by the sniffer.

30 The FW disallows any transmissions from the internal network to the rest of the Internet.

1.5.9.4. Message Bandwidth

35 A transaction authorization request requires about 400 bytes and registration packets require about 2 KB. To handle 1000 transaction authorizations per second and 1 registration packet per second, the FW

Machines are able to process about 400 KB per second (all known in the industry) .

Each DPC site requires an aggregate bandwidth of nearly three T1 connections to the third party modem bank and the other DPC sites.

1.5.10. Gateway Machine

1.5.10.1. Purpose

The GM Machine (GM), through the FW Machines, link the outside world (BIA-equipped terminals and other DPCs) to the internal components of the DPC. The DPC has multiple GMs, typically two.

1.5.10.2. Usage

The GM supervises the processing of each BIA request, communicates with the various DPC components as necessary, and sends the encrypted results of the request back to the sender. The software performing this task is called the Message Processing Module.

The GM logs all requests it receives and any warnings from components it communicates with. For example, the GM logs any emergency account accesses, sequence number gaps, and invalid packets.

Processing a request may require the GM to inform GMs at all other DPCs of a change in the DPC databases. When this happens, the GM runs a distributed transaction to update the remote databases.

Distributed transactions fall into two categories: synchronous and asynchronous. Synchronous distributed transactions require the GM to wait for the distributed transaction to commit before continuing to process the packet. Asynchronous distributed transactions do not require the GM to wait for the commit, and allow it to finish processing the request regardless of whether the distributed transaction commits or not. Asynchronous distributed transactions are only used to update data for which database consistency is not an absolute requirement: sequence numbers and biometric checksum recordings may be performed asynchronously, whereas creating database records, such as Individual Biometric records, may not.

When executing a synchronous distributed transaction, the requesting GM only considers the entire transaction successful if all sites can successfully commit the transaction locally. Otherwise, the GMs back out the changes locally and reject the request due to a transaction error.

The list of valid DPC sites is normally all of the sites. In the case of an extreme site failure, however, a system administrator may manually remove that site from the valid site list. The most likely cause of distributed transaction failures, however, are temporary network failures that are unrelated to any DPC equipment. Requests that require a synchronous distributed transaction cannot be performed until network connectivity is restored or the site is removed from the valid site list. Before a site can be added back to the valid site list, the system administrator brings the site's databases up to date with those of a currently active site.

1.5.10.3. Software Components

Each GM runs the following software components locally for performance reasons:

- Message Processing Module
- Message Authentication Code Module
- Message Decrypt Module
- Individual Biometric Database Machine List

1.5.10.4. Message Bandwidth

The message bandwidth required by the GMs is similar to that required by the FW Machines. A FDDI network interface provides 100 Mbits per second and easily covers any bandwidth requirements.

1.5.11 DPC LAN

1.5.11.1 Purpose

The DPC Local Area Network (LAN) links the machines of the DPC sites together using a fiber optic token ring. The fiber optic token ring provides both high bandwidth and good physical security.

1.5.11.2 Security

5 The network interfaces used by the machines on the DPC LAN include encryption hardware to make tapping or intercepting packets useless without the encryption key. The encryption key is the same for all machines on the LAN and is stored in the encryption hardware.

10 A properly configured network sniffer acts as an intruder detector as backup for the FW. If an anomalous message is detected, the intruding messages are recorded in their entirety, an operator is alerted, and the FW is physically shut down by the sniffer.

1.5.12 Message Processing Module

15 1.5.12.1 Purpose

The Message Processing Module (MPM) handles the processing for a request packet. It communicates with other components of the DPC as necessary to perform its tasks. The presence of an MPM on a machine brands it as a GM.

1.5.12.2 Usage

25 The MPM maintains a request context for each request it is currently processing. The request context includes the information necessary to maintain the network connection to the terminal making the request, the BIA device information, the response key, and the response packet.

30 1.5.13. Message Authentication Code Module

1.5.13.1. Purpose

35 The Message Authentication Code Module's (MACM) tasks are to validate the Message Authentication Code on inbound packets and to add a Message Authentication Code to outbound packets.

1.5.13.2. Usage

The MACM maintains an in-memory hash table of 112-bit MAC encryption keys keyed by BIA hardware identification code.

5 When the MACM receives a request from the GM to validate a packet's MAC, it first looks up the packet's hardware identification code in the hash table. If no entry exists, then the MACM replies to the GM with an "invalid hardware identification code" error.

10 Otherwise, the MACM performs a MAC check on the BIA message part of the packet using the 112-bit MAC encryption key. If the MAC check fails, then the MACM replies to the GM with an "invalid MAC" error. Otherwise, the MACM replies with a "valid MAC" message.

15 If the packet contains a merchant code, the MACM also checks the merchant code against the owner identification code in the hash table. If the codes don't match, then the MACM replies with an "invalid owner" error.

20 When the MACM receives a request from the GM to generate a MAC for a packet, it looks up the MAC encryption key using the packet's hardware identification code. With the MAC encryption key, the MACM generates a MAC and adds it to the packet. If the MACM cannot find the hardware identification code in its hash table, it replies with an invalid hardware identification code error instead.

1.5.13.3. Database Schema

25 The MACM hash table entry contains:

MACM Entry:

hardwareId = int4

ownerId = int4

macEncryptionKey = int16

30 The table is hashed by hardware identification code.

1.5.13.4. Database Size

5 Assuming 5 million BIA-equipped devices in service, the hash table requires about 120 MB of storage. For performance reasons, this hash table is cached completely in memory.

1.5.13.5. Dependencies

10 The MACM only contains records referencing active BIA hardware identification codes and active apparatus owners. Whenever an apparatus or apparatus owner is suspended or deleted from the system, the MACM removes any entries that reference the identification code. When an apparatus is activated, the MACM then adds an entry for it.

15 The MACM also caches the MAC encryption key from the Valid Apparatus Database. Since the system does not allow the encryption key of an BIA to be changed, the MACM does not need to worry about receiving encryption key updates.

1.5.14. Message Decrypt Module

1.5.14.1. Purpose

20 The Message Decrypt Module's (MDM) task is to reconstruct the DUKPT transaction key and with it decrypt the biometric- PIC block of the packet. It maintains a list of the DUKPT Base Keys that are required to generate the transaction key.

1.5.14.2. Usage

30 The MDM constructs the DUKPT transaction key using the packet's sequence number as the DUKPT transaction counter, the upper 22 bits of the BIA hardware identification code as the DUKPT tamper resistant security module (or "TRSM") Identification, and the low 10 bits of the BIA hardware identification code as the DUKPT Key Set Identification.

35 The DUKPT standard specifies how the transaction key is generated. The Key Set Identification is used to look up a Base Key from the

Base Key List. The Base Key is used to transform the TRSM Identification into the initial key via a DES encrypt/decrypt/encrypt cycle. The transaction counter is then applied to the initial key as a series of DES encrypt/decrypt/encrypt cycles to generate the transaction key.

For additional security, two Base Key Lists are maintained, one for low security BIA devices and one for high security devices. The MDM chooses which Base Key List to use depending on the security level of the device.

1.5.14.3. Database Schema

The MDM Base Key List entry contains:

MDM Entry:

baseKey = int 16

The Base Key List is indexed by Key Set Identification.

1.5.14.4. Database Size

The MDM maintains an in-memory list of the DUKPT Base Keys. Each key requires 112-bits. The MDM maintains two sets of 1024 keys requiring 32 KB total.

1.5.14.5. Dependencies

The MDM has no direct dependencies on any other DPC component.

1.5.15. PIC Group List

1.5.15.1. Purpose

The PIC Group List (PGL), in conjunction with the Individual Biometric Database Machine List, defines the configuration of the IBD machines. The PGL stores a list of the PIC groups in the system which is used to simplify the management of the PICs. A PIC group is a set of consecutive PIC codes. A PGL exists on each GM Machine (GM).

1.5.15.2. Usage

5 The PGL, when given a PIC code, searches through its list of PIC groups for the group containing the PIC code. The PGL maintains the list of groups in order and uses a binary search to quickly find the correct group.

The initial configuration for the PGL is one giant PIC group containing all possible PICs. After a threshold number of PICs are assigned, the giant PIC group is split in two. Thereafter, this process is applied to all succeeding PIC groups.

10 When a PIC group splits, the PGL assigns a new main and backup IBD machine based on available storage on a first-come-first serve basis. The PGL coordinates with the IBD machines to first copy the affected records from the old main and backup machines to the new ones, update the IML record, and last remove the old main and backup copies. Splitting a PIC group is an involved task. The PGL batches split requests to be run when the DPC is lightly loaded, for instance, at night.

15 The system administrator may also change the main and backup IBD machines for a given PIC group if the machines' free storage falls below a level required for handling the expected amount of new registrations.

1.5.15.3. Database Schema

25 The schema for the PIC Group records are:

PICGroup:

lowPin = int8

highPin = int8

used = int4

30 Each PIC group is identified by a unique identifier. For convenience the PIC group identification code is the lowPin code for the group, however the system does not otherwise rely upon this fact.

35 The PGL is keyed by the lowPin field.

1.5.15.4. Database Size

5 The PGL is expected to contain about 3000 groups (each PIC group contains about 1000 active PICs, but may span millions of actual PICs). The entire PGL requires about 72 KB of storage and is cached completely in memory.

1.5.15.5. Dependencies

10 When PIC groups are added, merged, or split up, the PGL is responsible for informing the IBD Machine List of the changes and for directing the movement of IBD records from one IBD machine to another.

1.5.16. Individual Biometric Database Machine List

1.5.16.1. Purpose

15 The IBD Machine List (IML), in conjunction with the PIC Group List, codifies the configuration of the IBD machines. The IML maps a PIC code to the main and backup IBD machines storing IBD records for the PIC. The IML is actually keyed by PIC Group (a set of consecutive PIC codes) rather than by individual PICs because this greatly reduces the memory required to store the list. An IML exists on each GM Machine (GM).

1.5.16.2. Usage

20 When a GM processes a request that requires a biometric identification, the GM finds the IML record keyed by the biometric's PIC group. The GM then knows the main and backup IBD machines to use for the biometric identification.

25

30

1.5.16.3. Database Schema

The schema for the IML list entries are:

MachinePair:

pinGroup = int8

main = int2,

backup = int2

The IML is keyed by pinGroup.

1.5.16.4. Database Size

The IML is expected to contain about 3000 entries (the number of PIC Groups). Each MachinePair record is 12 bytes requiring about 36 KB of storage and is cached completely in memory.

1.5.16.5. Dependencies

Any changes in the configuration of the IBD machines are be reflected in the IML. In addition, the IML uses PIC groups for its keys so when the PIC Group List gets modified, the IML are also updated.

1.5.17. Sequence Number Module

1.5.17.1. Purpose

The Sequence Number Module's (SNM) primary function is to prevent replay attacks by validating packet sequence numbers. Its secondary task is to minimize the effects of a resubmission attack by informing other SNMs in remote DPC sites of sequence number updates and to periodically update the sequence numbers in the Valid Apparatus Database.

The SNM maintains an in-memory hash table of sequence numbers keyed by BIA hardware identification code codes to allow quick validation of packet sequence numbers.

1.5.17.2. Usage

5 When the SNM receives a validate request from the GM for a given hardware identification code and sequence number, it looks up the hardware identification code in the hash table. If no entry exists, then the SNM replies to the GM with an "invalid hardware identification code" error.

10 Otherwise, the SNM checks the given sequence number against the sequence number stored in the hash table entry. If the sequence number is less than or equal to the stored sequence number, the SNM replies with an "invalid sequence number" error. Otherwise, the SNM sets the sequence number in the hash table entry to the given sequence number and replies with a "valid sequence number" message.

15 From time to time, the SNM may observe a sequence number gap. A sequence number gap occurs when the SNM receives a sequence number that is more than one greater than the sequence number stored in the hash table entry. In other words, a sequence number was skipped. When the SNM discovers a sequence number gap, it replies with a "sequence number gap" message to the GM instead of a "valid sequence number" message. The GM treats the packet as valid, but it also logs a "sequence number gap" warning.

20 Sequence number gaps usually occur when network connectivity is lost: packets are dropped or can't be sent until the network is restored to working order. However, sequence number gaps occur for fraudulent reasons as well: malicious parties could intercept packets preventing them from arriving at the DPC or they could even attempt to counterfeit packets (with a large sequence number so that it isn't immediately rejected).

25 The SNM's secondary function is to inform other DPCs of the updated sequence numbers. Quickly updating sequence numbers at all DPC sites thwarts resubmission attacks wherein a malicious entity monitors packets whose destination is for one DPC site and immediately sends a copy to a different DPC site in the hope of exploiting the transmission delay of sequence number updates from one DPC site to another resulting in both sites accepting the packet as valid, when only the first site should accept the packet.

30 The SNMs send update messages to each other whenever they receive a valid sequence number. If an SNM receives an update message for a sequence number that is less than or equal to the sequence number currently

stored in its hash table, that SNM logs a sequence number resubmission warning. All resubmission attacks are detected in this manner.

5 A simpler way to thwart resubmission attacks completely, is to have only one SNM validate packets. Under this scheme, there is no update transmission delay window to exploit with a resubmission attack. Alternately, multiple SNMs can be active at the same time provided none of them handle sequence number validation for the same BIA-equipped device.

10 1.5.17.3. Sequence Number Maintenance

When the SNM boots up, it loads the sequence number hash table from the sequence numbers for active BIA stored in the VAD.

Once per day, the SNM downloads the current sequence numbers to the local Valid Apparatus Database (VAD).

15 The VAD is responsible for sending add-entry and remove-entry messages to the SNMs for any BIA-equipped devices that are activated or deactivated to keep the SNM hash table up-to-date.

20 1.5.17.4. Database Schema

The SNM hash table entry contains:

SNM Entry:

hardwareId = int4

sequenceNumber = int4

25 The hash table is keyed by hardwareId.

30 1.5.17.5. Database Size

Assuming about 5 million BIA-equipped devices in service requires the hash table to be about 40 MB.

1.5.17.6. Dependencies

5 The SNM depends on the Valid Apparatus Database. When an apparatus is suspended or removed from the database, the SNM removes the corresponding entry. When an apparatus is activated, the SNM creates an entry for it.

1.5.17.7. Message Bandwidth

10 The SNMs require a transmission bandwidth of about 8 KB per second to handle 1000 update sequence number messages per second. The update sequence number messages is buffered and sent out once per second to minimize the number of actual messages sent.

1.5.18. Apparatus Owner Database

1.5.18.1. Purpose

15 The Apparatus Owner Database (AOD) stores information on individuals or organizations that own one or more BIA-equipped devices. This information is used to double check that the BIA devices are used only by their rightful owners, to provide asset account information for financial credit and debit transactions, and to allow identification of all BIAs owned by a specific individual or organization.

1.5.18.2. Usage

20 Each AOD record includes an asset account to credit or debit the owner when the DPC processes a financial transaction submitted by one of the owner's BIA-equipped devices. For instance, transactions submitted from BIA attached to a retail point of sale terminal involves credits to the asset account, while certified electronic mail transmissions results in debits to the asset account.

25

30

1.5.18.3. Database Schema

The schema for the Apparatus Owner record is:

ApparatusOwner:

ownerId = int4
name = char50
address = char50
zipCode = char9
assetAccount = char16
status = int1

The status field is one of:

0: suspended
1: active

The Apparatus Owner Database is keyed by ownerId.

1.5.18.4. Database size

The AOD is expected to store about 2 million Apparatus Owner records. Each entry is 130 bytes requiring about 260 MB of storage. The AOD is stored as a hashed file keyed by owner identification code. A copy of the AOD is stored on each GM.

1.5.18.5. Dependencies

When entries are removed or suspended from the AOD, any Valid Apparatus Database records that reference those apparatus owners are marked as suspended. In addition, the MAC Module and the Sequence Number Module remove their entries for the suspended apparatuses.

1.5.19. Valid Apparatus Database

1.5.19.1. Purpose

The Valid Apparatus Database (VAD) is a collection of records representing all of the BIAs that have been manufactured to date. The VAD

record contains the Message Authentication Code encryption key for each BIA, as well as an indication of whether an BIA is active, awaiting shipment, or marked as destroyed. In order for a message from an BIA to be decrypted, the BIA must exist and have an active record in the VAD.

1.5.19.2. Usage

When manufactured, each BIA has a unique public identification code and a unique MAC encryption key, both of which are entered into the VAD record prior to BIA deployment.

When an BIA is first constructed, it is given a unique hardware identification code. When an BIA is placed in service, its hardware identification code is registered with the system. First, the owner or responsible party of the BIA is entered into the Apparatus Owner Database (AOD). Then, the VAD record is pointed to the AOD record, and the BIA is then set active. Requests from that BIA are accepted by the DPC.

When an BIA is removed from service, it is marked as inactive, and the link to the AOD record is broken. No communications from that BIA are accepted.

Each BIA type and model has a security level assigned to it that indicates its level of physical security. When the DPC processes requests from that BIA, it uses the BIA's security level to gauge what kind of actions are allowed. The DPC also provides the security level to external financial transaction authorization services.

For example, a financial transaction authorization service can decide to deny any request for over \$300 from low security BIA, requiring individuals to use higher security BIA to authorize such sums. The authorization service can also use the security level as a guide on how much to charge for the transaction, based on risk.

The security levels and the actions that they allow are determined operationally. Basically, the cost to defraud the system must be higher than the potential gain, so the security level is related to the cost to compromise the device.

1.5.19.3. Database Schema

The schema for the Valid Apparatus record is:

Valid Apparatus:

5 hardwareId = int4
macEncryptionKey = int16
ownerId = int8
mfgDate = time
10 inServiceDate = time
securityLevel = int2
status = int1
type = int1
use = int1

15 Possible values for the status field are:

0: suspended
1: active
2: destroyed

20 Possible values for the type field are (one for each type of terminal):

0: ATM
1: BRT
2: CET
3: CPT
25 4: CST
5: EST
6: IPT
7: IT
8: ITT
30 9: PPT
10: RPT
11: SFT

Possible values for the use field are:

- 0: retail
- 1: personal
- 2: issuer
- 3: remote

The Valid Apparatus Database is keyed by hardware identification code.

1.5.19.4. Database Size

The VAD handles about 5 million retail, issuer, and remote Valid Apparatus entries. Each entry is 51 bytes requiring about 255 MB total. The VAD is stored as a hashed file keyed by hardware identification code. A copy of the VAD is stored on each GM.

The number of personal Valid Apparatus entries number in the range of 30 million requiring another 1.5 GB of storage.

1.5.19.5. Dependencies

When a VAD record changes status, the MAC Modules and Sequence Number Modules are informed of its change in status. For instance, when an apparatus becomes active, the MACP and SNM adds an entry for the newly active apparatus. When an apparatus becomes inactive, the MACP and SNM remove their entry for the apparatus.

1.5.20. Individual Biometric Database

1.5.20.1. Purpose

Individual Biometric Database (IBD) records store information on individuals, including their primary and secondary biometrics, PIC code, list of financial asset accounts, private code, emergency account, address, and phone number. The individual may optionally include their SSN and electronic mail address. This information is necessary for identifying an individual either by biometric or personal information, for accessing account information, or for

providing an address or phone number to remote merchants for additional verification.

1.5.20.2. Usage

5
10
Individuals are added to the system during the individual enrollment process at registered Biometric Registration Terminals located in retail banking establishments worldwide, or in local system offices. During enrollment, individuals select their personal identification numbers, and add financial asset accounts to their biometric and PIC combination.

15
Individuals may be removed from the database due to fraudulent activity reported by any issuing member. If this occurs, the individual's account information is moved from the IBD to the Prior Fraud Database (PFD) by an authorized internal systems representative. The biometric Ids for records in the PFD may not be used for records in the IBD.

20
The IBD exists on multiple machines, each of which is responsible for a subset of the IBD records with a copy of each record stored on two different machines, both for redundancy and for load-sharing. The IBD Machine List, stored on the GM, maintains which machines hold which PICs.

1.5.20.3. Database Schema

The schema for the Individual Biometric record is:

IndividualBiometric:

25
30
35
primaryBiometric = biometric
secondaryBiometric = biometric
biometricId = int4
PIC = char10
phoneNumber = char12
lastName = char24
firstName = char24
middleInitial = char2
SSN = char9
privateCode = char40
address = char50
zipCode = char9

publicKey = char64
checksums = int4[10]
accountLinks = char30[10]
5 emergencyIndex = char1
emergencyLink = char1
privs = char10
enroller = int8
emergencyUseCount = int4
10 status = int1

The status field is one of:

- 0: suspended
- 1: active
- 15 2: priorFraud

The IBD is keyed by PIC.

1.5.20.4. Database Indexes

20 Each IBD machine has additional indexes on the individual's Social Security Number, biometric identification code, last name, first name, and phone number to facilitate access to the IBD database.

1.5.20.5. Database Size

25 Each IBD machine has 40 GB of secondary storage provided by one or more RAID devices. Each IBD record is 2658 bytes (assuming the biometrics are 1K apiece) allowing up to 15 million records per machine. The IBD records are stored using a (perhaps clustered) secondary index on the
30 PIC. The index is stored in memory and requires no more than 64 MB (a 64 MB index handles about 16 million entries). To store records for 300 million individuals, the DPC needs at least 40 IBD machines: 20 IBD machines for main storage and another 20 for backup. The number of IBD machines is easily
35 scaled up or down depending on the number of registered individuals.

1.5.20.6. Dependencies

5 The IBD machines, PIC Group List, and the IBD Machine List remain up-to-date in terms of which PICs are on which machine. When a PIC group is reconfigured or main and backup machines for PIC groups are changed, the IBD machines update their databases and indexes appropriately.

1.5.21. Authorized Individual Database

10 1.5.21.1. Purpose

For each issuer or personal BIA-equipped device, the Authorized Individual Database (AID) maintains a list of individuals who are authorized, by the owner of the device, to use it.

15 The AID exists for two reasons. The first is that it provides restricted access to a terminal. For example, the Issuer Terminal can only be used by an authorized bank representative. The second reason for the AID is to prevent criminals from secretly replacing the BIA in a retail point of sale terminal with that of a personal BIA from a phone Terminal and thus routing all purchases to a remote merchant account set up by the criminals.

20 1.5.21.2. Database Schema

The schema for the Authorized Individual record is:

25 Authorized Individual:

hardwareId = int4

biometricId = int4

30 The hardwareId refers to a record in the Valid Apparatus Database and the biometricId refers to a record in the Individual Biometric Database. Whenever the DPC needs to check whether an individual is authorized to use a personal or issuer BIA device, the DPC checks for the existence of an Authorized Individual record with the correct hardwareId and biometricId.

35 Personal BIA devices are identified by a use field set to 1 (personal) in the Valid Apparatus Database. Issuer BIA devices are identified by a use field set to 2 (issuer) in the Valid Apparatus Database.

1.5.21.3. Database Size

5 Assuming each issuer terminal has 10 individuals authorized to use it and an each personal device has 2 additional authorized individuals with 1,000,000 personal devices in the server, the AID stores about:

$$10 * 100,000 + 2 * 1,000,000 = 3,000,000 \text{ entries}$$

10 The entire database requires about 24 MB of storage.

1.5.21.4. Dependencies

15 When Authorized Owner Database records or Valid Apparatus Database records are removed, all Authorized Individual records referencing them are removed.

1.5.22. Prior Fraud Database

20 1.5.22.1. Purpose

25 The Prior Fraud Database (PFD) is a collection of records representing individuals who have defrauded member issuers at some point in the past. The PFD also runs background transactions during periods of low system activity to weed out individuals in the IBD who have matching records in the PFD.

30 The system does not automatically put individuals in the PFD, unless it detects that they are attempting to register again. Placing an individual in the PFD is a sensitive policy matter which is outside the scope of this document.

1.5.22.2. Usage

35 Before a new IBD record is marked as active, the individual's primary and secondary biometrics are checked against each and every biometric in the PFD using the same biometric comparison techniques as those

used in the individual identification procedure.. If a match is found for the new IBD record, the IBD record's status is set to "prior fraud". If the prior fraud check was executed as part of a registration request, the GM logs a "registering individual with prior fraud" warning.

It is assumed that the PFD will remain relatively small. The cost to run the PFD is expensive, as it is an involuntary biometric search, so it is important to add only those individuals to the PFD who have imposed a significant cost to the system.

1.5.22.3. Database Schema

The schema for the Prior Fraud record is:

Prior Fraud:

primaryBiometric = biometric
 secondaryBiometric = biometric
 biometricId = int4
 PIC = char10
 phoneNumber = char12
 lastName = char24
 firstName = char24
 middleInitial = char2
 SSN = char9
 privateSignal = char40
 address = char50
 zipCode = char9
 publicKey = char64
 checksums = int4[10]
 accountLinks = char30[10]
 emergencyIndex = char1
 emergencyLink = char1
 privs = char10
 enroller = int8
 emergencyUseCount = int4
 status = int1

The status field is one of:

0: suspended

1: active

2: prior fraud

5

The PFD is keyed by biometric identification code.

1.5.22.4. Database Size

10

The PFD record is the same as the IBD record. Fortunately, the DPC needs to store a lot less of them so only two database machines are required to store the entire database, of which one is the backup.

1.5.22.5. Dependencies

15

The PFD does not have any direct dependencies on any other DPC component.

1.5.23. Issuer Database

20

1.5.23.1. Purpose

25

The Issuer Database (ID) stores information on banks and other financial institutions that allow their asset accounts to be accessed through the system. The issuing institutions are the only entities that can add or remove their asset account numbers to a given individual's IBD record.

1.5.23.2. Usage

30

The DPC uses the ID to validate requests from Issuer Terminals by searching the ID for a record containing the Issuer Terminal's issuer code. The owner Identification stored in the record must match up with the owner stored in the Valid Apparatus Database for the BIA stored in the Issuer Terminal.

The schema for the Issuer record is:

Issuer Record:

issuerCode = int6

ownerId = int4

name = char50

phoneNumber = char12

address = char50

zipCode = char9

The Issuer Database is keyed by issuerCode.

1.5.23.3. Database Size

The Issuer Database handles about 100,000 entries. Each entry is 127 bytes requiring less than 2 MB. A copy of the ID is stored on each GM.

1.5.23.4. Dependencies

The Issuer Database does not have any direct dependencies on any other DPC component.

1.5.24. Electronic Document Database

1.5.24.1. Purpose

The Electronic Document Database (EDD) stores and tracks electronic documents such as fax images and electronic mail messages destined for specified individuals. It also maintains corporate organizational charts to provide the official titles of both sender and receiver. The EDD also archives the documents at the sender or receiver's request and provides a neutral, third-party verification of contract agreements submitted through the system.

1.5.24.2. Usage

When the DPC receives a fax or other electronic document from an individual, it creates an EDD Document record to store the document until it is picked up by the authorized recipients.

For fax documents, the recipients are specified by fax number and extension. For other electronic documents, the recipients are specified by electronic mail address. The DPC looks up an Organization record for each recipient by fax number and extension or e-mail address. If the record cannot be found, then the DPC looks in the Individual Biometric Database but only if the recipient is specified by e-mail address. For each recipient, the DPC creates a Recipient record that references both the Document and the recipient's biometric Identification specified by the Organization or IBD record if found. The DPC allows recipients who are not registered in the system, but it cannot then ensure delivery or confidentiality for those recipients.

The EDD is flexible enough to allow fax documents to be sent to an individual's e-mail address and e-mail messages sent to a fax machine.

While no electronic signature is placed on the document by the system, the system does guarantee through encryption that the message as received (and decrypted) by the Certified Email or Secure Fax terminal was sent by the individual.

Duly authorized officers of the organization can submit secure faxes or electronic messages to the DPC to assign title and fax extensions to new members, to update a member's title or fax extension, or to remove terminated members.

When an individual is removed from the organization tree, the DPC retires the extension number for a period of one year. This retirement period allows the individual sufficient time to inform confidants that he can no longer receive confidential faxes at that extension and so that the organization cannot mistakenly activate someone else at the extension who might then otherwise receive faxes not intended for him or her.

The EDD maintains an archive database which contains copies of Document and Recipient records when requested by the sender or one of the recipients of the document. The archive database is periodically moved onto CD-ROM.

1.5.24.3. Database Schema

The EDD has three record types:

Document Record:

documentNumber = int8
senderId = int4
documentFax = fax
documentText = text
messageKey = int8
status = int 1

Recipient Record:

documentNumber = int8
recipientId = int4
recipientFaxNumber = char12
recipientFaxExtension = char8
recipientEmailAddr = text
receivedBy = int4
lastModified = time
deliveryStatus = int1
contractStatus = int1

Archive Request Record:

biometricId = int4
documentNumber = int8
requestorFaxNumber = char12
requestorFaxExtension = char8
requestorEmailAddr = text

Organization Record:

biometricId = int4
registeredBy = int4
company = text
title = text
faxNumber = char12
faxExtension = char8
emailAddr = text
activeDate = time
privs = int2
status = int 1

The Document record status field is one of:

0: incomplete

1: ok

The Recipient record delivery status field is one of:

0: incomplete

1: notified

2: rejected

3: retrieved

4: retrieved unsecured

5: busy

The Recipient record contract status field is one of:

0: none

1: accepted

2: rejected

The Organization record status field is one of:

0: active

1: suspended

The Organization record privs** field is used to indicate what privileges the DPC allows that individual:

0: registration

The Document, Recipient, and Archive Retrieve records are keyed by documentNumber. The Organization records are keyed by biometricId. The EDD maintains secondary indexes on the Document senderId field, the Recipient recipientId field, and the Organization company name and title fields.

1.5.24.4. Database Size

The EDD's storage requirements depend primarily on the number of fax pages it will have to store since e-mail messages are relatively small compared to fax pages. Each fax page requires about 110 KB of storage.

Assuming 4 pages per fax, 2 faxes per person per day, and 30 million fax machines, the EDD requires 24 GB of storage to spool one day's worth of faxes.

5 1.5.24.5. Security

Documents are sent to and from the system encrypted using the BIA encryption mechanism. However, the encryption key is stored in the same database as the document. The document is left in its encrypted form to prevent casual disclosure, but individuals concerned about security of documents stored on the system should make some arrangement for additional encryption themselves.

15 1.5.24.6. Message Bandwidth

Each fax page requires about 110 KB which means that a T1 connection, with a throughput of 1.54 MBits/second, can handle about 1.75 fax pages per second.

20 1.5.25. Electronic Signature Database

1.5.25.1. Purpose

25 The Electronic Signature Database (ESD) authenticates and tracks all electronic signatures created by the system.

1.5.25.2. Usage

30 Individuals who are members of the system submit a 16-byte "message digest" for the document along with biometric-PICs and obtain a "digital signature" which remains on file with the system in perpetuity. This digital signature encodes the individual's name, biometric identification code, the authorized signature record number, document title, along with the timestamp at which the document was signed.

To verify a signature, a message digest for the document are first calculated (using RSA's MD5 for instance) and sent along with the document's signature tags. The ESD looks up the signature tags and validates the just recently calculated message digest against the message digest stored in the database.

1.5.25.3. Database Schema

The schema for the Electronic Signature record is:

Electronic Signature:

signatureNumber = int8

signer = int4

documentName = text

checksum = int16

date = time

The signer is the biometric identification code for the individual signing the document. The electronic signature record is hashed by signatureNumber.

1.5.25.4. Database Size

For each 1 GB of secondary storage, the Electronic Signature Database stores 27 million records (each record is about 32 bytes).

1.5.25.5. Dependencies

The ESD has dependencies on the signer's biometric Identification. Since these signatures remain valid essentially forever, ESD records are not removed when the system deletes the signer's Individual Biometric Database record. Note that this requires the IBD to never reuse a biometric Identification.

1.5.26. Remote Merchant Database

1.5.26.1. Purpose

5 The Remote Merchant Database (RMD) stores information on
merchants that provide goods or services over telephones, cable television
networks, or the Internet. Each order sent by an individual using a
properly-equipped terminal is routed through the merchant's order terminal to
10 the system.

1.5.26.2. Usage

15 Once an individual's remote transaction authorization is received
and the MAC validated by the DPC, the merchant code is compared against
the merchant code in the RMD. The merchant code, be it phone number,
merchant-product credential, or internet address, exists in the RMD record
under the correct merchant identification code or the DPC terminates the
request and returns an invalid merchant code error to the sending BIA terminal
20 device.

1.5.26.3. Database Schema

The schema for the Remote Merchant record is:

Remote Merchant:

25 merchantId = int4
 merchantCode = char16
 merchantType = int1
 publicKey = int16

30 The Remote Merchant merchantType is one of:

 0: telephone
 1: CATV
 2: Internet

35 The merchantId and merchantCode are both primary keys. No two
RMD records have the same merchantId and merchantCode combination.

1.5.26.4. Database Size

5 Assuming about 100,000 remote merchants, the RMD requires about 24 bytes per record for a total of about 2.4 MB storage required.

1.5.26.5. Dependencies

10 The RMD does not have any direct dependencies on any other DPC components.

1.5.27. System Performance

15 The key performance number is how many financial authorization transactions the DPC handles per second.

In GM:

- 20 1. MACM checks the MAC (local)
2. SNM checks the sequence number (network message)
3. MDM decrypts the biometric-PIC block (local)
4. Find IBD machine (local)
5. Send identify request to the IBD machine (network message)

In IBD machine:

- 25 6. Retrieve all IBD records for the PIC (x seeks and x reads, where x is the number of pages required to store the biometric records).
- 30 7. For each record, compare against its primary biometric ($y / 2$ ms where y is the number of records retrieved).
8. If no reasonable match, repeat step 9 but compare against the secondary biometric ($z * y / 2$ ms, where y is the number of records retrieved and z is the probability no match is found).
- 35 9. Update the best matching IBD record's checksum queue and check for possible replay attacks (1 seek, 1 read, and 1 write).

10. Return the best matching IBD record or an error if the match is not close enough (network message).

In GM:

5

- 11. Authorize request with an external processor (network message)
- 12. GM encrypts and MACs the response (local).
- 13. Sends response packet back (network message).

10

Total Disk Costs:

$$x * (s + r) + y / 2 * (1 + z) + s + r + w + 5 * n$$

$$= (x + 1) * (s + r) + y / 2 * (1 + z) + w + 5 * n$$

[assume x is 20, y is 30, z is 5%; s = 10ms, r = 0ms, w = 0ms, n = 0ms]

= 21 * 10 ms + 15 * 1.05 ms

15

= 226 ms

= 4.4 TPS

[assume x is 10, y is 15, z is 5%; s = 10ms, r = 0ms, w = 0ms, n = 0ms]

= 11 * 10 ms + 7.5 * 1.05 ms

= 118 ms

20

= 8.4 TPS

[assume x is 1, y is 1, z is 5%; s = 10ms, r = 0ms, w = 0ms, n = 0ms]

= 2 * 10 ms + 1/2 * 1.05 ms

= 21 ms

25

= 47 TPS

The backup IBD machine also processes requests doubling effective TPS.

Worst case (with 2 machines in use):

30

Individuals per PIC	TPS
30	8
15	16
1	94

Average case (with 20 machines in use):

Individuals per PIC	TPS
30	88
15	168
1	940

Best case (with 40 machines in use):

Individuals per PIC	TPS
30	176
15	336
1	1880

The above is just an example of one configuration of the system as it could be implemented in a commercially viable manner. However, it is anticipated that this invention can be configured in many other ways which could incorporate the use of faster computers, more computers and other such changes.

1.6. Terminal Protocol Flowchart

The following set of protocol flows describe interactions between specific terminals, the DPC, the attached BIA, and other parties such as the credit/debit processor, and so on.

1.6.1. Retail Point of Sale Terminal

In this case, an RPT communicates with a retail BIA and the DPC to authorize a transaction. The transaction amount is 452.33, the individual's account is 4024-2256-5521-1212 merchant code is 123456, and the individual's private code is "I am fully persuaded of it."

- RPT → BIA Set Language <English>
- BIA → RPT Ok
- RPT → BIA Get Biometric <20>
- BIA/LCD: <Please place finger on lighted panel>
- Individual places finger on scanner

BIA → RPT Ok
 RPT → BIA Get Pin <40>
 BIA/LCD: <Please enter your PIC, then press <enter>>
 Individual enters PIC, then <enter>
 5 BIA → RPT Ok
 RPT → BIA Get Account Number <40>
 BIA/LCD: <Now enter your account index code, then press <enter>>
 Individual enters code, then <enter>
 BIA → RPT Ok
 10 RPT → BIA Validate Amount <452.33> <40>
 BIA/LCD: <Amount 452.33 OK?>
 Individual enters OK
 BIA → RPT Ok
 RPT → BIA Assign Register <1> <123456>
 15 BIA → RPT Ok
 RPT → Form Message <transaction>
 BIA → RPT <Transaction Request Message>
 BIA → RPT OK
 BIA/LCD: <I'm talking to DPC Central>
 20 RPT → DPC <Transaction Request Message>
 DPC: validate biometric, retrieve account number → 4024-2256- 5521-1212
 DPC → VISA <authorize 4024-2256-5521-1212 452.33 123456>
 VISA → DPC <ok 4024-2256-5521-1212 452.33 123456 autho-code>
 DPC: get private code
 25 DPC → RPT <Transaction Response Message>
 RPT → BIA Show Response <Transaction Response Message> <8>
 BIA/LCD: <Transaction ok: I am fully persuaded of it>
 BIA → RPT <Ok <autho-code>>
 RPT: prints receipt with autho-code on it
 30

1.6.2. Internet Point of Sale Terminal

In this case, an IPT communicates with a standard BIA and the
 DPC to authorize a transaction. The transaction amount is 452.33, the
 35 individual's account is 4024-2256-5521-1212, the internet merchant is located

at merchant.com, his merchant code is 123456, and the individual's private code is "I am fully persuaded of it."

5 IPT → merchant.com <send me merchant code if resources available>

merchant.com → IPT <ok 123456 merchant.com-public-key>

IPT generates session key, encrypted with merchant.com-public-key

IPT → merchant.com <session key>

All subsequent communications with merchant are encrypted with session key.

10 merchant.com → IPT <price and product information>

IPT/Screen: displays price and product information

Individual: selects item "fruitcake, price 45.33"

IPT → BIA Set Language <English>

BIA → IPT Ok

IPT → BIA Get Biometric <20>

15 BIA/LCD: <Please place finger on lighted panel>

Individual places finger on scanner

BIA → IPT Ok

IPT → BIA Get Pin <40>

BIA/LCD: <Please enter your PIC, then press <enter>>

20 Individual enters PIC, then <enter>

BIA → IPT Ok

IPT → BIA Get Account Number <40>

BIA/LCD: <Now enter your account index code, then press <enter>>

Individual enters code, then <enter>

25 BIA → IPT Ok

IPT → BIA Validate Amount <45.33> <40>

BIA/LCD: <Amount 45.33 OK?>

Individual enters OK

BIA → IPT Ok

30 IPT → BIA Assign Register <1> <123456>

BIA → IPT Ok

IPT → BIA Assign Register <2> <merchant.com>

BIA → IPT Ok

IPT → BIA Assign Register <3> <fruitcake>

35 BIA → IPT Ok

IPT → BIA Form Message <remote transaction>

BIA → IPT <Remote Transaction Request Message>

BIA → IPT OK

BIA/LCD: <I'm talking to DPC Central>

IPT → merchant.com <Remote Transaction Request Message>

merchant.com → secure-connect to DPC using DPC public key

merchant.com → DPC <Remote Transaction Request Message>

DPC: validate biometric, retrieve account number → 4024-2256- 5521-1212

DPC: validate internet merchant.com with code 123456

DPC → VISA <authorize 4024-2256-5521-1212 45.33 123456>

VISA → DPC <ok 4024-2256-5521-1212 45.33 123456 autho- code>

DPC: get private code

DPC → merchant.com <Transaction Response Message>

merchant.com stores autho code

merchant.com → IPT <Transaction Response Message>

IPT → BIA Show Response <Transaction Response Message> <8>

BIA/LCD: <Transaction ok: I am fully persuaded of it>

BIA → IPT <Transaction ok>

1.6.3. Internet Teller Terminal

In this case, an ITT communicates with a standard BIA, the DPC, and a bank's internet server to perform routine and nonroutine home banking operations. Note that the DPC isn't involved in actually validating any transactions, but is only responsible for creating a valid set of network credentials and securing the communications line to the bank.

ITT → bank.com <send me bank code if resources available>

bank.com → ITT <ok 1200>

ITT → BIA Set Language <English>

BIA → ITT Ok

ITT → BIA Get Biometric <20>

BIA/LCD: <Please place finger on lighted panel>

Individual places finger on scanner

BIA → ITT Ok

ITT → BIA Get Pin <40>

BIA/LCD: <Please enter your PIC, then press <enter>>

Individual enters PIC, then <enter>

BIA → ITT Ok

RPT → BIA Get Account Number <40>

BIA/LCD: <Now enter your account index code, then press <enter>>

5

Individual enters code, then <enter>

BIA → ITT Ok

ITT → BIA Assign Register <1> <1200> (bank code)

BIA → ITT Ok

ITT → BIA Assign Register <2> <bank.com>

10

BIA → ITT Ok

ITT → BIA Assign Register <3> <ITT.port, bank.com.port> (TCP/IP addresses)

BIA → ITT Ok

ITT → Form Message <net credential>

BIA → ITT <network credential Request>

15

BIA → ITT Ok

BIA/LCD: <I'm talking to DPC Central>

ITT → DPC <network credential Request>

DPC: validate biometric, create credential(time, acct, bank)

DPC: get private code

20

DPC → ITT <network credential Response>

ITT → BIA Show Response <network credential Response>

BIA decrypt response, check response

BIA/LCD: <Credential ok: I am fully persuaded of it>

BIA encrypt credential, session key, challenge key with bank's public key

25

BIA → ITT <Secure Connection Request Message>

BIA → ITT <Session Key>

BIA → ITT Ok

BIA/LCD: <Secure connection to bank.com in progress>

ITT → bank.com <Secure Connection Request Message>

30

bank.com decrypt with private key, validate credential, use shared key

bank.com → ITT <ok>

Further transactions over the ITT → bank.com connections are all encrypted by the ITT using the ITT/bank session key.

35

Any transactions that the bank determines are non-routine must be validated by the individual using the BIA's challenge-response mechanism.

The challenge-response mechanism is available only while the BIA remains in the "secure connection" state.

5 bank.com → ITT <validate <validation request>>
 ITT → BIA Validate Private <encrypted validation request>
 BIA decrypts challenge section, and displays it
 BIA/LCD: <Please OK: transfer of 12,420.00 to 1023-3302- 2101-1100>
 Individual enters Ok
 BIA re-encrypts response using challenge key
 10 BIA/LCD: <Secure connection to bank.com in progress>
 BIA → ITT <Ok <encrypted validation response>>
 ITT → bank.com <encrypted validation response>

1.6.4. Electronic Signature Terminal

15 In this case, an EST communicates with a standard BIA and the DPC to construct digital signatures. The individual's private code is "I am fully persuaded of it" and the document to be signed is called "The Letter of Marque."

20 CET → BIA Set Language <English>
 BIA → CET Ok
 CET → BIA Get Biometric <20>
 BIA/LCD: <Please place finger on lighted panel>
 25 Individual places finger on scanner
 BIA → CET Ok
 CET → BIA Get Pin <40>
 BIA/LCD: <Please enter your PIC, then press <enter>>
 Individual enters PIC, then <enter>
 30 BIA → CET Ok
 CET → BIA Validate Document <Letter of Marque> <40>
 BIA/LCD: <Document "Letter of Marque" OK?>
 Individual enters OK
 BIA → CET Ok
 35 CET → BIA Assign Register <1> <document MD5 value>
 BIA → CET Ok

CET → Form Message <signature submit>
 BIA → CET <Electronic Signature Request>
 BIA → CET OK
 BIA/LCD: <I'm talking to DPC Central>
 5 CET → DPC <Electronic Signature Request>
 DPC: validate biometric, create signature, return sig text code
 DPC: get private code
 DPC → CET <Electronic Signature Response>
 CET → BIA Show Response <Electronic Signature Response> <8>
 10 BIA/LCD: <Document ok: I am fully persuaded of it>
 BIA → CET <Ok <sig text code>>

1.6.5. Certified Email Terminal

15 In this case, a CET communicates with a standard BIA and the
 DPC to transmit certified electronic mail. The individual's private code is "I
 am fully persuaded of it", and the document name is "Post Captain."

20 CET → BIA Set Language <English>
 BIA → CET Ok
 CET → BIA Get Biometric <20>
 BIA/LCD: <Please place finger on lighted panel>
 Individual places finger on scanner
 BIA → CET Ok
 25 CET → BIA Get Pin <40>
 BIA/LCD: <Please enter your PIC, then press <enter>>
 Individual enters PIC, then <enter>
 BIA → CET Ok
 CET → BIA Validate Document <Post Captain> <40>
 30 BIA/LCD: <Document "Post Captain" OK?>
 Individual enters OK
 CET/Screen: <Recipient list? >
 Individual enters <fred@telerate.com joe@reuters.com>
 35 CET → BIA Assign Register <1> <fred@telerate.com joe@reuters.com>
 BIA → CET Ok
 CET → Form Message <document submit>

BIA → CET <Electronic Document Submit Request>

BIA → CET OK

BIA/LCD: <I'm talking to DPC Central>

CET → DPC <Electronic Document Submit Request>

5 DPC: validate biometric, create message, return message #001234

DPC: get private code

DPC → CET <Electronic Document Submit Response>

CET → BIA Show Response <Electronic Document Submit Response> <8>

BIA/LCD: <Document ok: I am fully persuaded of it>

10 BIA → CET <Document ok <1234>>

CET → DPC <Electronic Document Data Request, 1234, section 1, incomplete>

DPC → CET <Electronic Document Data Response, incomplete>

CET → DPC <Electronic Document Data Request, 1234, section 2, incomplete>

DPC → CET <Electronic Document Data Response, incomplete>

15 CET → DPC <Electronic Document Data Request, 1234, section 3, incomplete>

DPC → CET <Electronic Document Data Response, incomplete>

CET → DPC <Electronic Document Data Request, 1234, section 4, done>

DPC → CET <Electronic Document Data Response, track 1234.1 1234.2>

DPC → fred@telerate.com <email 1234.1 message arrived>

20 DPC → joe@reuters.com <email 1234.2 message arrived>

mailer@telerate.com → DPC <received notification email for 1234.1>

DPC → sender@company.com <email 1234.1 recipient notified>

mailer@reuters.com → DPC <received notification email for 1234.2>

DPC → sender@company.com <email 1234.2 recipient notified>

25

[At Fred's CET: Fred sees the "message arrived" electronic mail message, and decides to go pick up the message]

CET → BIA Set Language <English>

30 BIA → CET Ok

CET → BIA Get Biometric <20>

BIA/LCD: <Please place finger on lighted panel>

Individual places finger on scanner

BIA → CET Ok

35 CET → BIA Get Pin <40> BIA/LCD: <Please enter your PIC>

Individual enters PIC, then <enter>

BIA → CET Ok
 CET → BIA Assign Register <1> <1234.1>
 BIA → CET Ok
 CET → Form Message <document retrieve>
 5 BIA → CET <Electronic Document Retrieve Request>
 BIA → CET OK
 BIA/LCD: <I'm talking to DPC Central>
 CET → DPC <Electronic Document Retrieve Request>
 DPC: validate biometric, lookup 1234.1
 10 DPC: get private code
 DPC → CET <Electronic Document Retrieve Response>
 CET → BIA Show Response <Electronic Document Retrieve Response> <8>
 BIA/LCD: <Document ok: I am fully persuaded of it>
 BIA → CET <Document ok <message key>>
 15 CET/Screen: decrypt, then show document

1.6.6. Secure Fax Terminal

20 In this case, a SFT communicates with an BIA/catv and the DPC to
 transmit secure faxes.

SFT → BIA Get Biometric <20>
 BIA/LCD: <Please place finger on lighted panel>
 Individual places finger on scanner
 25 BIA → SFT Ok
 BIA/LCD: <Please enter your PIC, then press <enter>>
 Individual enters PIC, then <enter>
 SFT → BIA Set Pin <40>
 BIA/LCD: <Please enter your Title Index, then press <enter>>
 30 Individual enters title index, then <enter>
 SFT → BIA Set Title Index Code <40>
 BIA → SFT Ok
 SFT/Screen: <Recipient? (add * for ext, # at end)>
 Individual enters <1 510 944-6300*525#>
 35 SFT/Screen: <Recipient? (add * for ext, # at end)>
 Individual enters <1 415-877-7770#>

SFT/Screen: <Recipient? (add * for ext, # at end)>
 Individual enters <#>
 SFT → BIA Assign Register <1> <15109446300*525 14158777770>
 BIA → SFT Ok
 5 SFT → Form Message <document submit>
 BIA → SFT <Secure Fax Submit Request>
 BIA → SFT OK
 BIA/LCD: <I'm talking to DPC Central>
 SFT → DPC <Secure Fax Submit Request>
 10 DPC: validate biometric, create message, return message #001234
 DPC: get private code
 DPC → SFT <Secure Fax Submit Response>
 SFT → BIA Show Response <Secure Fax Submit Response> <10>
 BIA/LCD: <Document ok: I am fully persuaded of it>
 15 BIA → SFT <Document ok <001234>>
 SFT → DPC <Secure Fax Data Request, 1234, section 1, incomplete>
 DPC → SFT <Secure Fax Data Response, incomplete>
 SFT → DPC <Secure Fax Data Request, 1234, section 2, incomplete>
 DPC → SFT <Secure Fax Data Response, incomplete>
 20 SFT → DPC <Secure Fax Data Request, 1234, section 3, incomplete>
 DPC → SFT <Secure Fax Data Response, incomplete>
 SFT → DPC <Secure Fax Data Request, 1234, section 4, done>
 DPC → SFT <Secure Fax Data Response>
 DPC → connect-fax 15109446300
 25 DPC → SFT6300 <fax-cover "Sam Spade" from "Fred Jones" 1234.1 4 pages waiting>
 DPC → disconnect
 DPC → connect-fax 14158777770
 DPC → SFT7770 <fax-cover "John Jett" from "Fred Jones" 1234.2 4 pages waiting>
 DPC → disconnect
 30
 [At Sam's SFT: Sam sees document fax cover arrive from Fred, initiates retrieval
 of document from DPC using tracking code 1234.1.]
 SFT → BIA Get Biometric <20>
 35 BIA/LCD: <Please place finger on lighted panel>
 Individual (Sam) places finger on scanner

BIA → SFT Ok
 SFT → BIA Get Pin <40>
 BIA/LCD: <Please enter your PIC, then press <enter>>
 Individual (Sam) enters PIC, then <enter>
 5 BIA → SFT Ok
 SFT → BIA Assign Register <1> <1234.1>
 BIA → SFT Ok
 SFT → Form Message <document retrieve>
 BIA → SFT <Secure Fax Retrieve Request>
 10 BIA → SFT OK
 BIA/LCD: <I'm talking to DPC Central>
 SFT → DPC <Secure Fax Retrieve Request>
 DPC: validate biometric, lookup 1234.1, verify biometric-PIC = Sam Spade
 DPC: lookup private code in database
 15 DPC → SFT <Secure Fax Retrieve Response>
 SFT → BIA Show Response <Secure Fax Retrieve Response> <8>
 BIA → SFT <Document ok: I am fully persuaded of it <message key>>
 SFT/Screen: <Document ok: I am fully persuaded of it>
 SFT/Screen: print fax
 20

1.6.7. Biometric Registration Terminal

In this case, a BRT communicates with a registration BIA and the DPC to register an individual with the system.

25 BRT → BIA Set Language <English>
 BIA → BRT Ok
 BRT → BIA Get Biometric <20> <primary>
 BIA/LCD: <Please place PRIMARY finger on lighted panel>
 30 Individual places primary finger on scanner
 BIA → BRT Ok
 BRT → BIA Get Biometric <20> <secondary>
 BIA/LCD: <Please place SECONDARY finger on lighted panel>
 Individual places secondary finger on scanner
 35 BIA → BRT Ok
 BRT → BIA Get Pin <40>

BIA/LCD: <Please enter your PIC, then press <enter>>
Individual enters 123456, then <enter>
BIA → BRT Ok
BRT → BIA Get Message Key
5 BIA → BRT <Ok <message key>>
BIA → <Registration Request Message>
BRT/Screen: <Name: >
Representative enters <Fred G. Shultz>
BRT/Screen: <Address: >
10 Representative enters <1234 North Main>
BRT/Screen: <Zipcode: >
Representative enters <94042>
BRT/Screen: <Private code: >
Representative queries individual, then enters <I am fully persuaded of it.>
15 BRT/Screen: <Asset account list: >
Representative enters <2, 1001-2001-1020-2011> (credit card)
Representative enters <3, 1001-1002-0039-2212> (checking account)
BRT/Screen: <Emergency account: >
20 Representative enters <1, 1001-1002-0039-2212> (emergency, checking
account)
BRT → Form Message <registration>
BIA → BRT <Registration Request Message>
BIA → BRT OK
BIA/LCD: <I'm talking to DPC Central>
25 BRT appends message-key-encrypted personal information to request
BRT → DPC Registration Request Message <encrypted personal information>
DPC: verify PIC 123456
DPC → BRT <Registration Response Message>
BRT → BIA Show Response <Registration Response Message> <8>
30 BIA/LCD: <Registration ok: I am fully persuaded of it, 123456>
BIA → BRT <Ok>

1.6.8. Customer Service Terminal

In this case, a CST communicates with a standard BIA and the DPC to verify the identity and the credentials of an individual.

5

CST → BIA Set Language <English>

BIA → CST Ok

CST → BIA Get Biometric <20>

BIA/LCD: <Please place finger on lighted panel>

10

Individual places finger on scanner

BIA → CST Ok

CST → BIA Get Pin <40>

BIA/LCD: <Please enter your PIC, then press <enter>>

Individual enters PIC, then <enter>

15

BIA → CST Ok

CST → BIA Get Message Key

BIA → CST <Ok <message key>>

CST → Form Message <Individual Identity Request>

20

BIA → CST <Individual Identity Request>

BIA → CST OK

BIA/LCD: <I'm talking to DPC Central>

CST → DPC <Individual Identity Request>

DPC: get private code, individual's priv

25

DPC → CST <Individual Identity Reply>

CST → BIA Show Response <Individual Identity Reply> <8>

BIA/LCD: <Identity ok: I am fully persuaded of it>

BIA → CST <Ok <individual-name priv>>

CST: check priv to see if sufficient for CST use

30

1.6.9. Issuer Terminal

In this case, an IT communicates with a standard BIA and the DPC to authorize and send a batch of account addition and deletion requests to the DPC. The individual's private code is "I am fully persuaded of it", and the bank code is 1200.

35

IT → BIA Set Language <English>
 BIA → IT Ok
 IT → BIA Get Biometric <20>
 5 BIA/LCD: <Please place finger on lighted panel>
 Individual places finger on scanner
 BIA → IT Ok
 IT → BIA Get Pin <40>
 BIA/LCD: <Please enter your PIC, then press <enter>>
 10 Individual enters PIC, then <enter>
 BIA → IT Ok
 IT → BIA Assign Register <1> <1200>
 BIA → IT Ok
 IT → BIA Get Message Key
 15 BIA → IT <message key>
 BIA → IT Ok
 IT → BIA Form Message <issuer request>
 BIA → IT <Issuer Batch Request>
 BIA → IT OK
 20 BIA/LCD: <I'm talking to DPC Central>
 IT → DPC <Issuer Batch Request> <message-key-encrypted issuer batch>
 DPC: validate biometric, validate bank code 1200 vs. BIA identification
 DPC: get private code
 DPC: decrypt message using message key, execute issuer batch
 25 DPC → IT <Issuer Batch Reply>
 IT → BIA Show Response <Issuer Batch Reply> <8>
 BIA/LCD: <Batch ok: I am fully persuaded of it>
 BIA → IT <Ok>

30 1.6.10. Automated Teller Machinery

In this case, an ATM communicates with an integrated ATM BIA and the DPC to identify an individual and obtain his bank account number. The individual's account is 2100-0245-3778-1201, bank code is 2100, and the individual's private code is "I am fully persuaded of it."

ATM → BIA Get Biometric <20>

ATM/LCD: <Please place finger on lighted panel>

Individual places finger on scanner

BIA → ATM Ok

ATM/LCD: <Please enter your PIC, then press <enter>>

Individual enters 123456 on ATM keyboard, then <enter>

ATM → BIA Set Pin <123456>

BIA → ATM Ok

ATM/LCD: <Now enter your account index code, then press <enter>>

Individual enters 2, then <enter>

ATM → BIA Set Account Index Code <2>

BIA → ATM Ok

ATM → BIA Assign Register <1> <2100>

BIA → ATM Ok

ATM → Form Message <account access>

BIA → ATM <Account Access Request Message>

BIA → ATM OK

ATM/LED: <I'm talking to DPC Central>

ATM → DPC <Account Access Request Message>

DPC: validate biometric, retrieve account number →2100- 0245-3778-1201

DPC: get private code

DPC → ATM <Account Access Response Message>

ATM → BIA Decrypt Response <Account Access Response Message>

BIA → ATM <2100-0245-3778-1201> <no emergency> <I am fully persuaded of it>

ATM/LCD: <I am fully persuaded of it>

At this point, the ATM has the account number it needs to continue, so it then retrieves the information associated with the account number, and commences interacting with the individual.

1.6.11. Phone Point of sale Terminal

In this case, a PPT communicates with an integrated phone BIA and the telephone merchant to download information and purchase items securely using the telephone. The individual's PIC is 1234, the account index

code is 1, the merchant's phone number is 1 800 542-2231, merchant code 123456, and the actual account number is 4024-2256-5521- 1212.

Note that the telephone strips the area code (1-800) from the telephone number before handing it to the system.

Individual dials phone 18005422231

PPT → connect merchant 18005422231

PPT → BIA Assign Register 1 <5422231>

Sales rep answers. Individual selects item "fruitcake". Sales rep downloads info. merchant → PPT <123456 fruitcake 43.54>

PPT → BIA Get Biometric <20>

Phone/LCD: <Please place finger on lighted panel>

Individual places finger on scanner

BIA → PPT Ok

Phone/LCD: <Please enter your PIC, then press #>

Individual enters 1234 on keypad, then # or * (enter)

PPT → BIA Set Pin <1234>

BIA → PPT Ok

Phone/LCD: <Now enter your account index code>

Individual enters 1, then <enter>

RPT → BIA Set Account index code <1>

BIA → PPT Ok

RPT → BIA Assign Register <2> <123456>

BIA → PPT Ok

Phone/LCD: <Press # if amount 45.54 is ok>

Individual enters # (yes)

PPT → BIA Set Amount <43.54>

BIA → PPT Ok

PPT → Form Message <remote transaction>

BIA → PPT <Remote Transaction Request>

BIA → PPT Ok

Phone/LCD: <I'm talking to DPC Central>

PPT → merchant <Phone Transaction Request>

merchant → DPC secure-connect to DPC using DPC-public-key

merchant → DPC <Phone Transaction Request>

DPC: validate biometric, retrieve account number → 4024-2256-5521-1212

DPC: validate merchant 5422231 has code 123456

DPC → VISA <authorize 4024-2256-5521-1212 43.54 123456>

VISA → DPC <ok 4024-2256-5521-1212 43.54 123456 autho- code>

5 DPC: get private code

DPC → merchant <Transaction Response Message>

merchant examines response code

merchant → PPT <Transaction Response Message>

PPT → BIA Decrypt Message <Transaction Response Message>

10 BIA → PPT <Ok <I am fully persuaded of it> <autho-code>>

Phone/LCD: <chime> Transaction ok: I am fully persuaded of it

1.6.12. Cable-TV Point of sale Terminal

15 In this case, a CPT communicates with an integrated cable-tv BIA and the Cable television merchant to download information and purchase items securely using the cable television broadband network. The individual's PIC is 1234, the account index code is 1, the channel is 5, the merchant code 123456, and the actual account number is 4024-2256-5521-1212.

20 Individual turns the television to channel 5.

merchant → CPT <fruitcake 43.54 123456> (broadcast)

Individual hits "buy" on TV Remote

CPT/TV: <Buying fruitcake for \$43.54>

25 CPT → BIA Get Biometric <20>

CPT/TV: <Please place finger on lighted panel>

Individual places finger on scanner

BIA → CPT Ok

CPT/TV: <Please enter your PIC, then press <enter>>

30 Individual enters 1234 on keypad, then "buy"

CPT → BIA Set Pin <1234>

BIA → CPT Ok

CPT/TV: <Now enter your account index code>

Individual enters 1, then <enter>

35 RPT → BIA Set Account index code <1>

BIA → CPT Ok

RPT → BIA Assign Register <1> <channel 5, 15:30:20 PST>
 BIA → RPT Ok
 CPT → BIA Assign Register <2> <123456>
 BIA → CPT Ok
 5 CPT/TV: <Press "buy" if amount 45.54 is ok>
 Individual enters "buy"
 CPT → BIA Set Amount <43.54>
 BIA → CPT Ok
 CPT → Form Message <CableTV transaction>
 10 BIA → CPT <CableTV Transaction Request>
 BIA → CPT Ok
 CPT/TV: <I'm talking to DPC Central>
 CPT → CTV Center <CableTV Transaction Request>
 CTV Center → merchant <CableTV Transaction Request>
 15 merchant → DPC secure-connect to DPC using DPC-public-key
 merchant → DPC <CableTV Transaction Request>
 DPC: validate biometric, retrieve account number → 4024-2256- 5521-1212
 DPC: validate merchant channel 5, current show has code 123456
 DPC → VISA <authorize 4024-2256-5521-1212 43.54 123456>
 20 VISA → DPC <ok 4024-2256-5521-1212 43.54 123456 autho- code>
 DPC: get private code, mailing address
 DPC → merchant <Transaction Response Message>
 merchant examines response code, records mailing address
 merchant → CTV Center <Transaction Response Message>
 25 CTV Center → CPT <Transaction Response Message>
 CPT → BIA Decrypt Message <Transaction Response Message>
 BIA → CPT <Ok <I am fully persuaded of it> <autho-code>>
 CPT/TV: <chime> Transaction ok: I am fully persuaded of it

30 From the foregoing, it will be appreciated how the objects and
 features of the invention are met.

35 First, the invention provides a computer identification system that
 eliminates the need for a user to possess and present a physical object, such as
 a token, in order to initiate a system access request.

Second, the invention provides a computer identification system that is capable of verifying a user's identity, as opposed to verifying possession of proprietary objects and information.

5 Third, the invention verifies the user's identity based upon one or more unique characteristics physically personal to the user.

Fourth, the invention provides an identification system that is practical, convenient, and easy use.

10 Fifth, the invention provides a system of secured access to a computer system that is highly resistant to fraudulent access attempts by non-authorized users.

Sixth, the invention provides a computer identification system that enables a user to notify authorities that a particular access request is being coerced by a third party without giving notice to the third party of the notification.

15 Seventh, the invention provides an identification system that allows for identification of the sender and recipient of an electronic message and/or facsimile.

20 Although the invention has been described with respect to a particular tokenless identification system and method for its use, it will be appreciated that various modifications of the apparatus and method are possible without departing from the invention, which is defined by the claims set forth below.

25

5. GLOSSARY

ACCOUNT INDEX CODE:

5 A digit or an alpha-numeric sequence that corresponds to a particular financial asset account

AID:

10 Authorized Individual Database: contains the list of individuals authorized to use personal and issuer BIA devices.

AOD:

Apparatus Owner Database: central repository containing the geographic and contact information on the owner of each BIA.

ASCII:

15 American Standard Code for Information Interchange

ATM:

20 Automated Teller Machinery; uses encoded biometric identity information to obtain access to a financial asset management system, including cash dispensing and account management.

BIA:

25 Biometric input apparatus; collects biometric identity information, encodes and encrypts it, and makes it available for authorizations. Comes in different hardware models and software versions.

Biometric:

30 A measurement taken by the system of some aspect of an individual's physical person.

Biometric ID:

35 An identifier used by the system to uniquely identify an individual's biometric record (IRID – Individual Record ID)

BIO-PIC GROUP:

A collection of algorithmically dissimilar biometric samples linked to the same personal identification code

BRT:

Biometric Registration Terminal; located at retail banking outlets, BRTs combine biometric registration information with an individual-selected PIN and selected personal information to register individuals with the system.

CBC:

Cipher Block Chaining: an encryption mode for the DES.

CCD:

Charged-Coupled Device

CET:

Certified Email Terminal; uses BIA to identify sender, encrypts document, sends to system. System retains, notifies recipient of message arrival in-system. Recipient identifies self, and then document is transmitted to recipient. Notification to transmitter once document is sent. Document is verified sent, secured by BIA encryption. Transmitter may inquire as to delivery status. Both participants must be system members.

COMMANDS:

A program or subroutine residing in the DPC that performs a specific task, activated by a request message sent from a BIA-equipped terminal.

CONTRACT ACCEPT/REJECT:

The process by which an individual enters their BIO-PIC and instructs the DPC to register said individual's contractual acceptance or rejection of the terms contained within a document which had been sent by electronic facsimile to that individual.

CPT:

5 Cable-TV Point-of-Sale Terminal: combines an onscreen display simulcast digital signal informing TV-top cable box of product information with product video, and an BIA controller remote which performs the biometric-pin validation using the CATV communications network. Order/autho/mailling-address/item-id forwarded to merchant. Results of authorization are displayed on the TV.

CST:

10 Customer Service Terminals; provide system customer service personnel with varying degrees of access (based on access privilege) the ability to retrieve and modify information on individuals in order to help people with account problems.

DATA SEALING STEP:

15 The conversion of plain text to cipher text (known as "encryption") in combination with the encrypted checksumming of a message that allows information to remain in plain text while at the same time providing a means for detecting any subsequent modification of the message.

DES:

20 Digital Encryption Standard: a standard for the cryptographic protection of digital data. See standard ANSI X3.92-1981

DETERMINATION:

25 The status of the command processed during the execution step.

DPC:

30 A data processing center, namely, the place and the entity where the hardware, software, and personnel are located with the goal of supporting a multigigabyte biometric identity database. A DPC processes electronic messages, most of which involve performing biometric identity checks as a precursor to performing some action, such as a financial transfer, or sending a fax, or sending
35 electronic mail, etc.

DSP:

Digital Signal Processor: a class of integrated circuits that specialize in the mathematical operations required by the signal processing applications.

5

DUKPT:

Derived Unique Key Per Transaction: See standard ANSI/ABA X9.24-1992

10

EDD:

Electronic Document Database: central repository containing all pending faxes and electronic messages awaiting pickup by individuals.

15

EMERGENCY ACCOUNT INDEX:

The alpha-numeric digit or sequence selected by an individual which, when accessed, will result in a transaction being labeled by the system as an emergency transaction, potentially causing the display of false screens and/or the notification of authorities that said individual has been coerced into performing a transmission or transaction.

20

ESD:

Electronic Signature Database: central repository containing all MD5 and electronic signatures of all documents signed by anybody, referenced by authorization number.

25

EST:

Electronic Signature Terminal; uses BIA to identify individual, computer calculates checksum on document, sends checksum to system, system validates, timestamps, saves checksum, and returns with sig code. Uses Internet as transport. EST also verifies signatures given a sig code and an MD5 calculation.

30

FAR (False Accept Rate):

The statistical likelihood that one individual's biometric will be incorrectly identified as the biometric of another individual.

35

FALSE SCREENS:

5 Displays of information which has been intentionally pre-determined to be subtly inaccurate such that a coercing party will not illegally obtain accurate data about an individual's financial assets, all the while remaining unaware of the alteration of the information.

FDDI:

10 Fiber Digital Device Interface: a networking device that utilizes a fiber optic token ring.

FS:

Field Separator

FW:

15 Firewall Machine: the internet-local net router that regulates traffic into and out of the DPC.

GM:

20 Gateway Machine: the main processing computers in the DPC; runs most of the software.

IBD:

25 Individual Biometric Database: central repository for biometric, financial asset, and other personal information. Queries against the biometric database are used to verify identity for transaction authorizations and transmissions.

ID:

30 Issuer Database: central repository containing the institutions that are allowed to add and delete financial asset account numbers with the system.

IML:

35 IBD Machine List: a software module in the DPC determines which IBD machines are responsible for which PIN codes.

INTERNET MERCHANT:

A retail account selling services or good to consumers by means of the Internet electronic network

IPT:

Internet Point-of-Sale Terminal: items and merchant code from the internet, BIA biometric-PIN for validation, sent to system using Internet, autho/order/PO # forwarded to merchant. System response using internet as well, displaying results on screen.

ISSUER:

A financial account issuer for financial assets to be registered with the DPC.

ISSUER BATCH:

A collection of "add" and "delete" instructions complete with biometric IDs, financial asset accounts, and account index codes verified and submitted by an issuer to the DPC.

IT:

Issuer Terminals; provides a batch connection to the system for issuers to add and remove (their own) financial asset account numbers from specific individual's IBD records.

ITT:

Internet Teller Terminal; authorizes network terminal session using encrypted credential obtained from DPC using biometric ID.

LCD:

Liquid Crystal Display: a technology used for displaying text.

MAC:

Message Authentication Code: an encrypted checksum algorithm, the MAC provides assurance that the contents of a message have not been altered subsequent to the MAC calculation. See standard ANSI X9.9-1986

5

MACM:

Message Authentication Code Module: a software module in the DPC that handles MAC validation and generation for inbound and outbound packets.

10

MDM:

Message Decrypt Module: a software module in the DPC that encrypts and decrypts packets from or destined to an BIA device.

15

MPM:

Message Processing Module: a software module in the DPC that performs the processing of request packets.

NETWORK CREDENTIAL:

Both the individual and the bank are identified by the DPC to create the network credential. The credential includes the individual's identification as well as the context of the connection (i.e., the TCP/IP source and destination ports). DPC creates a network credential using the individual's account id, the time of day, and the bank code. The DPC signs this credential using Public Key Encryption and the DPC's Private Key.

20

25

PFD:

Prior Fraud Database: central repository for IBD records which have had prior fraud associated with them. Every new customer's biometrics are checked against all PFD records with the intent of reducing recidivism.

30

PGL:

PIN Group List: a software module in the DPC that is responsible for maintaining the configuration of the IBD machines.

35

PIN:

Personal Identification Number; a method for protecting access to an individual's account through secret knowledge, formed from at least one number.

5

PIC:

Personal Identification Code; a PIN formed from either numbers, symbols, or alphabetic characters.

10

POS:

Point-Of-Sale; a place where goods are sold.

PPT:

Phone Point-of-Sale Terminal; combines phone number with merchant price and product information to authorize a transaction over a BIA-equipped telephone. Order/authorization/mailling-address/PO forwarded to merchant. Resulting authorization is displayed on phone LCD, or "spoken", along with the individual's private code.

15

20

RAM:

Random Access Memory

RF:

Radio Frequency: generally refers to radio frequency energy emitted during the normal operation of electrical devices.

25

REGISTERS:

Memory reserved for a specific purpose, data set aside on chips and stored operands to instructions

30

REQUESTS:

Electronic instructions from the BIA to DPC instructing the DPC to identify the individual and thereby process the individual's command in the event the identification is successful

35

RMD:

Remote Merchant Database: contains all merchant identification codes for merchant telephone and Cable TV order shops; indexed by merchant ID. Contains per-merchant system encryption codes as well.

5

RPT:

Retail Point-of-Sale Terminal; combines encoded biometric identity information with retail transaction information (possibly from an electronic cash register) and formulates authorization requests of the system using X.25 networks, modems, etc.

10

SECURE TRANSMISSION:

An electronic message or facsimile wherein at least one party has been identified by the DPC.

15

SFT:

Secured Fax Terminal; uses BIA to identify sender, sends fax either unsecured, sender-secured, secured, or secured-confidential. The latter two require recipients to identify themselves using biometric-PIN. Uses "titles" (specified using a title index digit) to label outbound faxes. Sender may inquire as to delivery status. Both participants must be system members. Either sender or recipient can request that the fax be archived.

20

25

SNM:

Sequence Number Module: a software module in the DPC that handles the DUKPT sequence number processing for inbound request packets. Sequence number processing protects against replay attacks.

30

Terminal:

A device that uses the BIA to collect biometric samples and form request messages that are subsequently sent to the DPC for authorization and execution. Terminals almost always append ancillary information to request messages, identifying counterparties and the like.

35

TITLE INDEX CODE:

Alpha-numeric sequence uniquely identifying an individual's authorized role or capacity within the context of his employment

5

Token:

An inanimate object conferring a capability.

TRACKING CODE:

10

An alpha-numeric sequence assigned to data stored in or transmitted by the DPC, such that said sequence may be used to recall the data or obtain a report on the status of the transmission of the data.

TRANSACTION:

15

An electronic financial exchange

TRANSMISSION:

An electronic message other than an electronic financial exchange

VAD:

20

Valid Apparatus Database: central repository in which each BIA (with associated unique encryption codes) is identified, along with the owner of the BIA.

25

I claim:

1. A voluntary tokenless identification computer system for determining an individual's identity from an examination of at least one biometric sample and a personal identification code gathered during a bid step, and comparison with previously recorded biometric sample and personal identification code gathered during a registration step, said system comprising:
 - a. at least one computer;
 - b. first gathering and display means for voluntary input of at least one biometric sample, personal identification code, and private code from an individual during the registration step, wherein the private code is selected by the individual;
 - c. second gathering and display means for voluntary input of at least one biometric sample and personal identification code, from an individual during a bid step;
 - d. first interconnecting means for interconnecting said first and second gathering and display means to said computer for transmitting the gathered biometric sample, personal identification code, and private code from said first and second gathering means to said computer;
 - e. means for comparison of biometric sample and personal identification code gathered during the bid step with the biometric sample and personal identification code gathered during the registration step, for producing an evaluation;
 - f. execution means within said computer for storage of data and processing and execution of commands for producing a determination; and
 - g. means for output of said evaluation, determination, or private code from said computer.
2. The apparatus of claim 1 wherein the computer comprises means for detecting and preventing electronic intrusion of the computer system.
3. The apparatus of claim 1 wherein the computer is placed remote from the gathering and display means.
4. The apparatus of claim 1, the first and second gathering and display means further comprising:
 - a. at least one biometric input means for gathering biometric samples further comprising a hardware and software component;
 - b. at least one terminal means that is functionally partially or fully integrated with the biometric input means for input of and appending additional data;

- 5
- c. at least one data entry means for input of a personal identification code where in said means is integrated either with the biometric input means or the terminal means; and
- d. second interconnecting means for interconnecting said biometric input means, data entry means and said terminal.
- 10
5. The apparatus of claim 4 wherein said terminal further comprises at least one display means for display of data.
6. The apparatus of claim 4 wherein the biometric input means has a hardware identification code previously registered with the computer, which makes the biometric input means uniquely identifiable to the computer.
- 15
7. The apparatus of claim 4 wherein the hardware component further comprises:
- a. at least one computing module for data processing;
- b. erasable and non-erasable memory modules for storage of data and software;
- c. biometric scanner device for input of biometrics data;
- d. data entry means for entering data;
- e. digital communication port; and
- f. means for prevention of electronic eavesdropping.
- 20
8. The apparatus of claim 7 wherein the computing modules are connected in a manner to prevent monitoring of communications between said computing modules.
9. The apparatus of claim 7 wherein the hardware component further comprises display means for display of data.
- 25
10. The apparatus of claim 7 wherein the hardware component further comprises RF shielding .
11. The apparatus of claim 4 wherein the hardware component further comprises a wireless communications means.
12. The apparatus of claim 7 wherein the biometric input means is secured from physical tampering.
- 30
13. The apparatus of claim 12 further comprising means for detection of physical penetration of the biometric input means.
14. The apparatus of claim 13 further comprising means for electronic self destruction whereby software and data stored within the memory module are erased.
15. The apparatus of claim 13 further comprising means for physical self destruction whereby the computing modules and memory modules are destroyed.
- 35
16. The apparatus of claim 4 wherein the hardware component further comprises means for reading magnetic strip cards.

17. The apparatus of claim 4 wherein the hardware component further comprises means for reading a smart card.
18. The apparatus of claim 4 wherein the software component resides in a computing module and further comprises;
- 5 a. electronically erasable memory module wherein at least one command interface module, a first set of software and associated data specifically configured for the intended use of the biometric input device and data are stored; and
- b. non-erasable memory module wherein a second set of software and
- 10 associated data are stored.
19. The apparatus of claim 18 said software component further comprising means for encryption of data from plaintext to ciphertext.
20. The apparatus of claim 18 said software component further comprising means to detect alteration of data further comprising;
- 15 a. a secret key; and
- b. an irreversible one way transformation of the data that cannot be reproduced without the secret key.
21. The apparatus of claim 18 wherein the first set of software and associated data further comprising:
- 20 a. biometric encoding algorithm; and
- b. encryption code.
22. The apparatus of claim 18 wherein the second set of software and associated data further comprising:
- 25 a. an operating system; and
- b. at least one device driver.
23. The apparatus of claim 4 wherein said terminal is any electronic device and which issues commands to and receives results from the biometric input means.
24. The apparatus of claim 23 wherein said terminal is selected from the group of facsimile machines, telephones, television remote control, personal computers, credit/debit card processors, cash registers, automated teller machines, wireless personal computers.
- 30 25. The apparatus of claim 4 wherein said second interconnecting means is means for wireless communications.
26. The apparatus of claim 1 wherein said first interconnecting means is selected from the group X.25, ATM network, Telephone network, Internet network, cable television
- 35 network, cellular telephone network.

27. The apparatus of claim 1 wherein the comparison means further comprises means for encryption and decryption of data.
28. The apparatus of claim 1 wherein comparison means further comprises means for identifying the biometric input device.
- 5 29. The apparatus of claim 1 wherein the computer system further comprises:
- a. at least one independent computer network system; and
 - b. third interconnecting means for interconnecting said computer system with said counter party computer system.
- 10 30. The apparatus of claim 29 wherein the third interconnecting means comprises an X.25 network.
31. The apparatus of claim 1 wherein the execution means comprises at least one database for storage and retrieval of data.
32. The apparatus of claim 31 wherein the data base further comprises an individual biometric data base.
- 15 33. The apparatus of claim 31 wherein the data base further comprises a prior fraud check data base.
34. The apparatus of claim 31 wherein the data base further comprises an electronic document data base.
- 20 35. The apparatus of claim 31 wherein the data base further comprises an electronic signature data base.
36. The apparatus of claim 1 wherein said output means is selected from the group of an X.25 network, ATM network, Telephone network, Internet network, cable television network.
- 25 37. The apparatus of claim 1 wherein said private code is generated by the computer.
38. A method for voluntary and tokenless identification of individuals, and authentication of the identification, said method comprising the steps of:
- a. registration step wherein at least one biometric sample, personal identification code, and private code from an individual is gathered and stored;
 - 30 b. bid step wherein at least one biometric sample and personal identification code from an individual is gathered;
 - c. comparison step wherein the biometric sample and personal identification code gathered during the bid step is compared with the biometric sample and personal identification code gathered and stored during the registration step, for producing either a successful or failed identification result;
- 35

- d. execution step wherein a command is processed and executed to produce a determination;
 - e. output step wherein said identification result or determination is externalized and displayed; and
 - 5 f. presentation step wherein on successful identification of the individual, the private code is presented to the individual being identified.
39. The method of claim 38 wherein both the registration and bid steps further comprise a biometric sample check step wherein the quality of the biometric sample is verified.
- 10 40. The method of claim 38 wherein the registration step further comprises a personal identification code and biometric sample duplication check step wherein the biometrics and personal identification code gathered during the registration step is checked against all previously registered biometrics currently associated with the identical personal identification code.
- 15 41. The method of claim 38 wherein the registration step further comprises an ancillary data input step wherein ancillary data is collected.
42. The method of claim 41 wherein the ancillary data further comprises name and address of the individual.
43. The method of claim 41 wherein the ancillary data further comprises a title of an individual.
- 20 44. The method of claim 43 wherein the ancillary data input step further comprises a title index assignment step wherein each title of the individual is assigned a code.
45. The method of claim 41 wherein the ancillary data further comprises a financial asset account number.
- 25 46. The method of claim 45 wherein the ancillary data input step further comprises an account index assignment step wherein each financial asset account number is assigned an index code.
47. The method of claim 38 wherein the registration step further comprises a prior fraud check step wherein the biometric sample gathered during registration is compared to a subset of previously registered biometric samples.
- 30 48. The method of claim 38 wherein the registration step further comprises an emergency mechanism setup step.
49. The method of claim 48 further comprising an emergency account index assignment step wherein an account index is labeled as an emergency account where in the event the account is accessed appropriate authorities are notified of the emergency.
- 35 50. The method of claim 49 further comprising a false screen display setup step wherein there is assignment of false screen data.

51. The method of claim 49 wherein access to various financial asset accounts is limited.
52. The method of claim 38 wherein the registration step further comprises a modification step wherein any previously entered ancillary data can be modified or deleted.
53. The method of claim 38 wherein both the registration and bid steps further comprise a data sealing step to provide the ability to detect alteration of the data further comprising;
- a. a secret key; and
 - b. an irreversible one way transformation of the data that cannot be reproduced without the secret key.
54. The method of claim 38, wherein the registration and bid steps further comprise an encryption step to convert the data from plaintext to ciphertext.
55. The method of claim 38 wherein the bid or registration steps further comprise a transmission step wherein the data is transmitted.
56. The method of claim 38 wherein the bid or registration steps is further provided with a unique transmission code having a unique hardware identification code and incrementing sequence number which increases by one for each transmission.
57. The method of claim 38 wherein the registration step further comprises choosing a language for communication in a set language step.
58. The method of claim 38 wherein the bid step further comprises choosing a title in a set title number step.
59. The method of claim 38 wherein the bid step further comprises choosing an account number in a set account number step.
60. The method of claim 38 wherein the bid step further comprises validating an amount in a validate amount step.
61. The method of claim 38 wherein the bid step further comprises entering an amount in an enter amount step.
62. The method of claim 38 wherein the bid step further comprises validating a document in a validate document step.
63. The method of claim 38 wherein the bid step further comprises appending ancillary data in an assign register step.
64. The method of claim 63 the ancillary data further comprising a counter party identification code.
65. The method of claim 38 wherein the bid or registration step further comprise aborting or canceling said step in a reset step.
66. The method of claim 38 wherein the bid step further comprises transmission of data in a transmission step.

67. The method of claim 38 wherein the bid step further comprises choosing a language for communication in a set language step.
68. The method of claim 38 wherein the comparison step further comprises use of the unique transmission codes to detect repeat transmissions.
- 5 69. The method of claim 38 wherein the comparison step further comprises a counter party identification step using the counter party identification and unique transmission codes.
70. The method of claim 38 wherein the comparison step comprises matching the individual's personal identification code and biometric gathered during the bid step, with the personal identification code and biometric gathered during the registration step for positive identification of the individual.
- 10 71. The method of claim 70 wherein if there is no match of the personal identification code and biometric gathered during the registration step and the personal identification code and biometric gathered during the bid step, there is no recognition of the individual.
- 15 72. The method of claim 38 wherein the execution step further comprises a debit/credit transaction step.
73. The method of claim 72 wherein the debit/credit transaction step further comprises an address collection step.
74. The method of claim 38 wherein the execution step further comprises an archiving step and a tracking code assignment step for archival of data.
- 20 75. The method of claim 74 wherein the data is sent through a message digest encoding algorithm step to produce an electronically signed document.
76. The method of claim 38 wherein the execution step further comprises the retrieval of archived data using said tracking code.
- 25 77. The method of claim 38 wherein the execution step further comprises a modification step wherein the title index code, account numbers and account index codes are added, deleted or modified.
78. The method of claim 38 wherein the execution step further comprises an account number retrieval step where the account index code is used to retrieve an account number.
- 30 79. The method of claim 38 wherein the execution step further comprises an emergency activation step.
80. The method of claim 79 wherein the emergency activation step further comprises recognition of the emergency code and identifying the entire transaction as an emergency and notification of authorities.
- 35

81. The method of claim 79 wherein the execution step further comprises a false display step wherein previously designated, false accounts or false limitations on accounts are accessible.
82. The method of claim 38 wherein the output step further comprises an identification result notification step.
83. The method of claim 38 wherein the output step further comprises a determination notification step.
84. The method of claim 38 wherein the output step further comprises an emergency code step wherein authorities are notified.
85. The method of claim 38 wherein the output step further comprises display of false screens.
86. The method of claim 38 wherein the presentation step further comprises encryption, externalization, and decryption of the private code.
87. A method for rapid search of at least one first previously stored biometric sample from a first individual, using a personal identification code-basket that is capable of containing at least one algorithmically unique second biometric sample from at least one second individual, and which is identified by said personal identification code-basket, comprising:
- a. a storage step further comprising:
 - i. selection of a personal identification code by said first individual;
 - ii. entering a biometric sample from said first individual;
 - iii. locating the personal identification code-basket identified by the personal identification code selected by said first individual;
 - iv. comparison of the biometric sample taken from said first individual, with any previously stored biometric samples in said selected personal identification code-basket, to make sure that the biometric sample entered by said first individual is algorithmically unique from the previously stored at least one biometric sample provided by at least one second individual; and
 - v. storage of the entered biometric sample from said first individual in the selected personal identification code-basket if said sample is algorithmically unique from the at least one previously stored biometric sample from said at least one second individual; and
 - b. a bid step further comprising:
 - i. entering said selected personal identification code by said first individual; and

- ii. entering a biometric sample by said first individual; and
- c. a comparison step further comprising:
 - i. finding the personal identification code-basket that is identified by said personal identification code entered by said first individual; and
 - ii. comparison of the entered biometric sample from said first individual with said at least one stored biometric sample from said at least one second individual in said entered personal identification code-basket for producing either a successful or failed identification result.

5

10

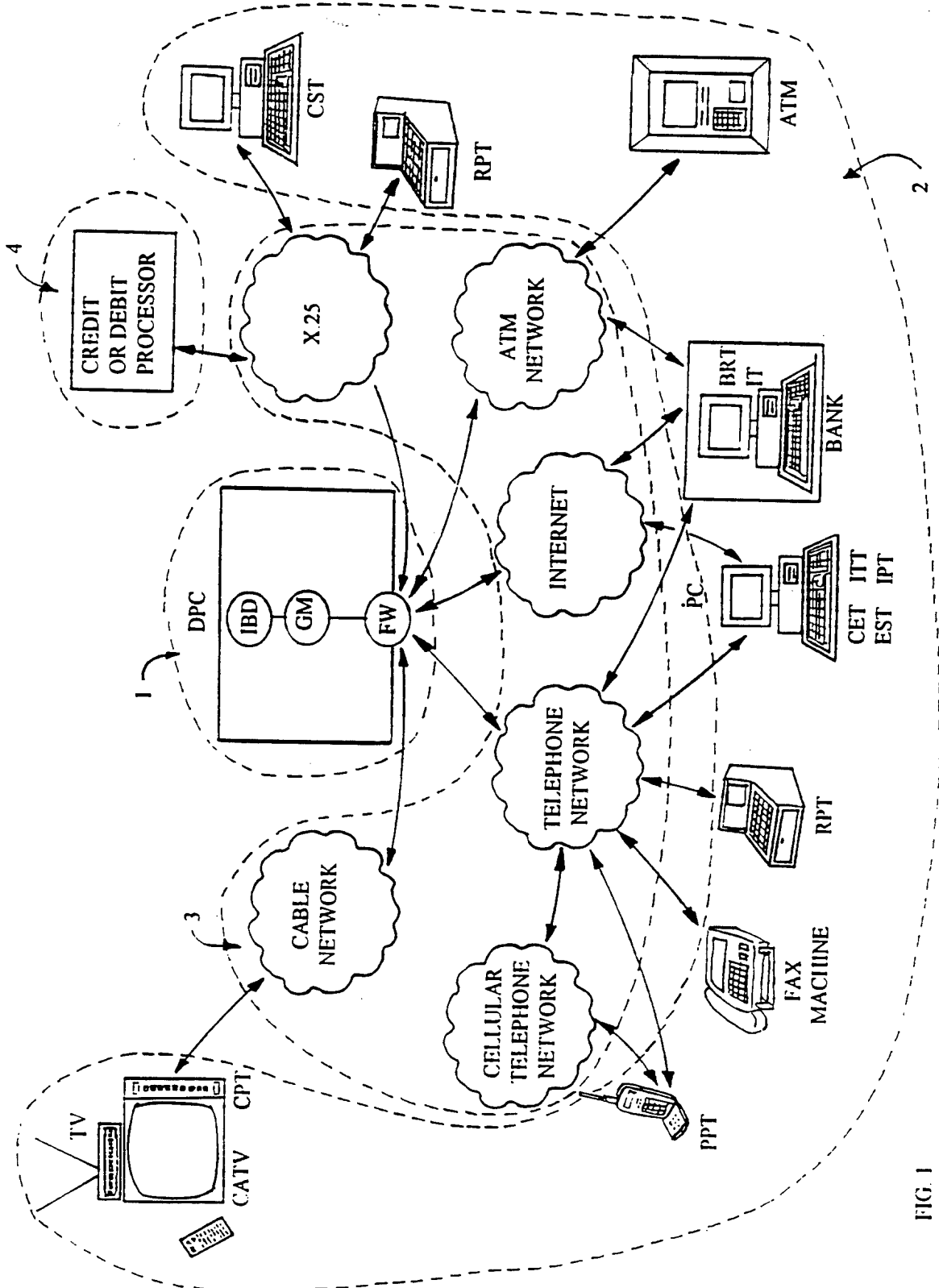


FIG. 1

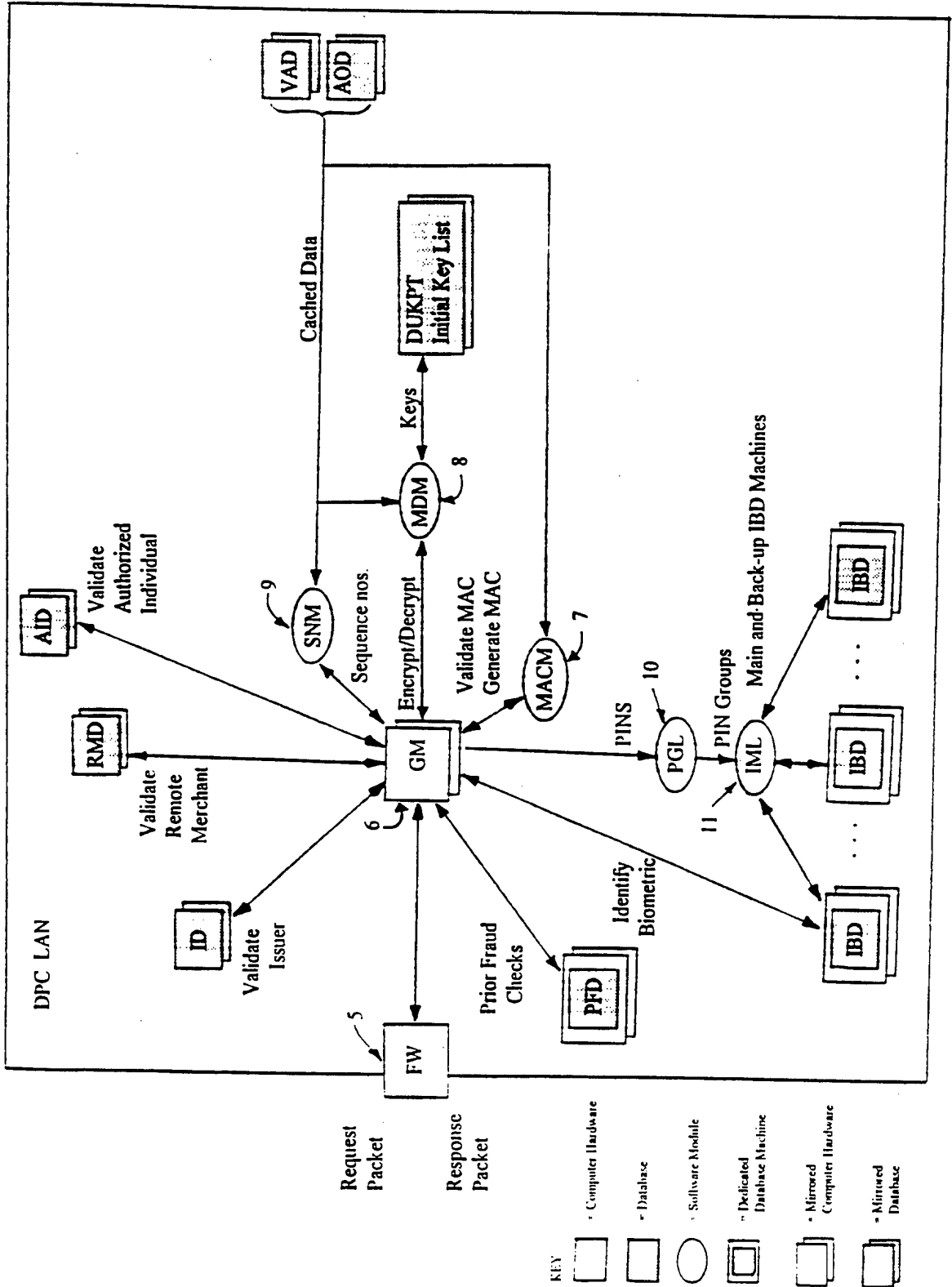


FIG. 2

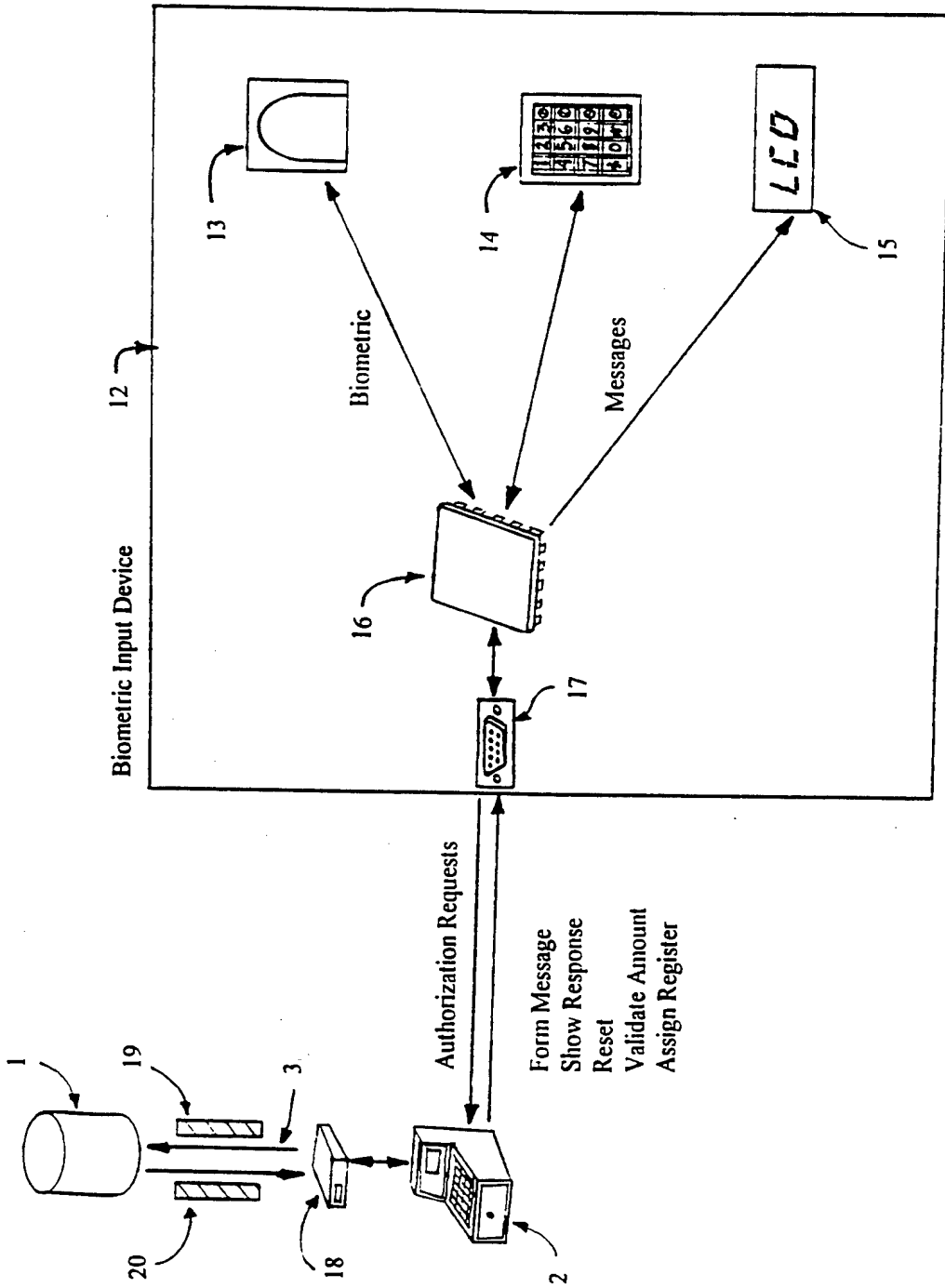


FIG. 3

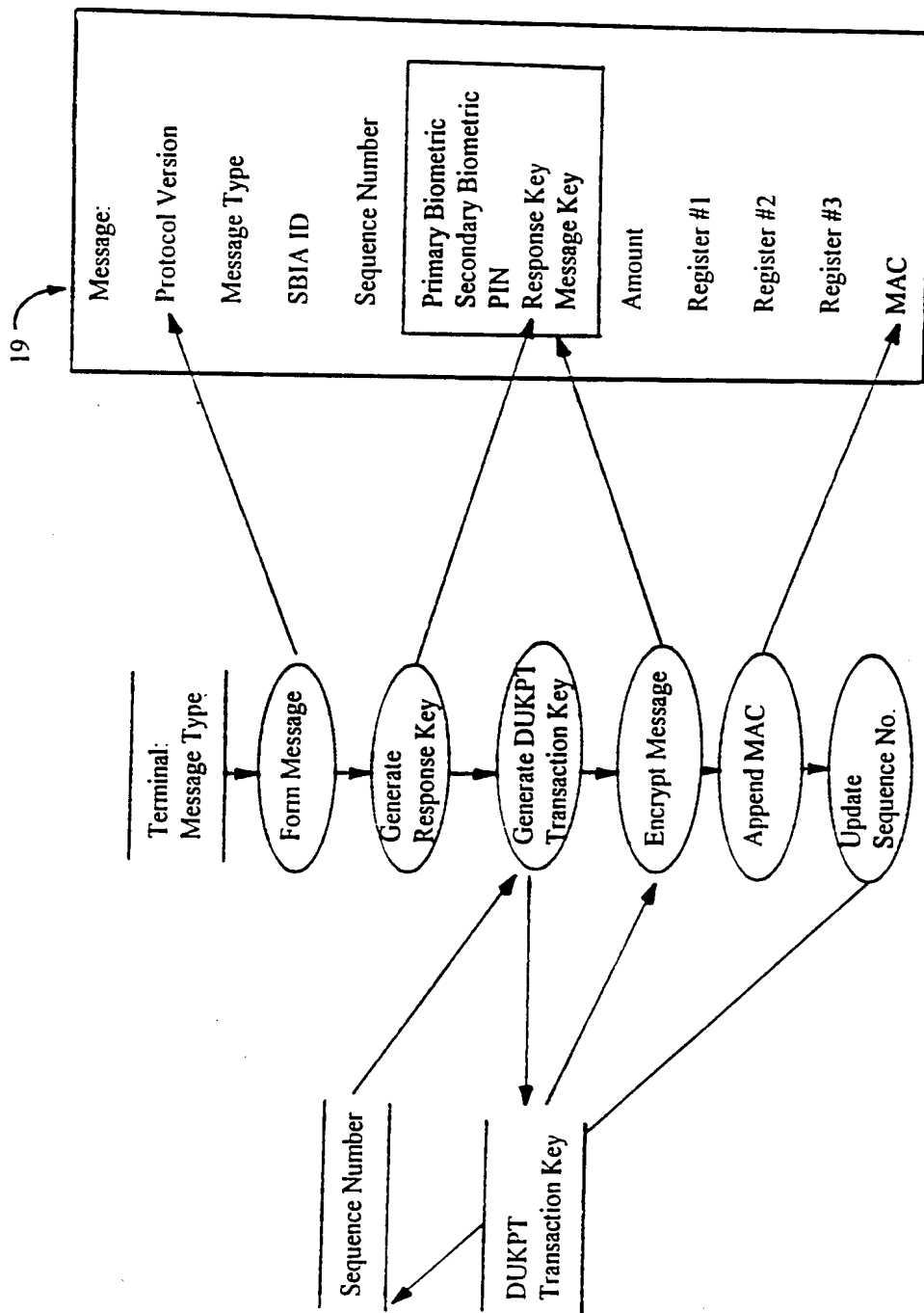


FIG. 4

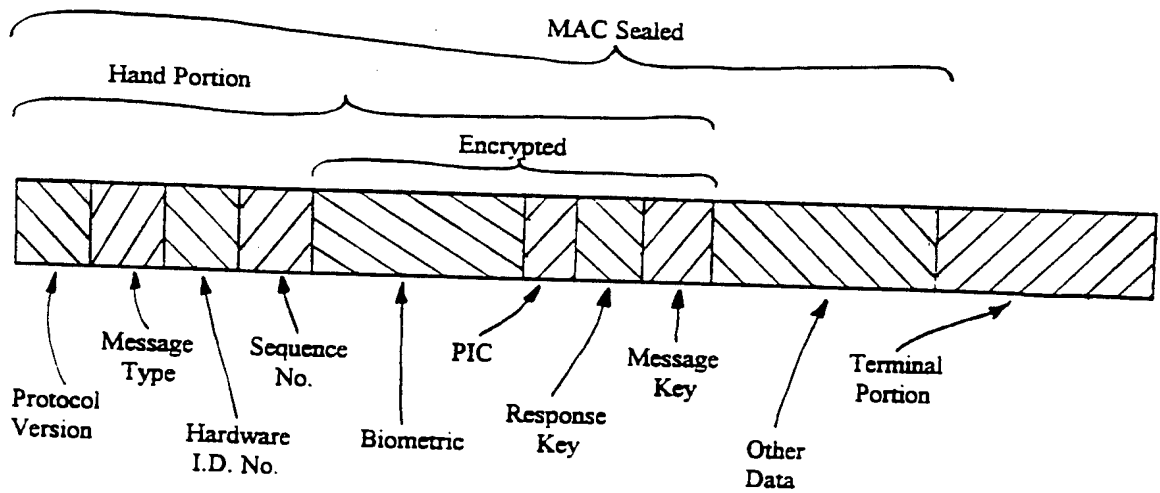


FIG. 5

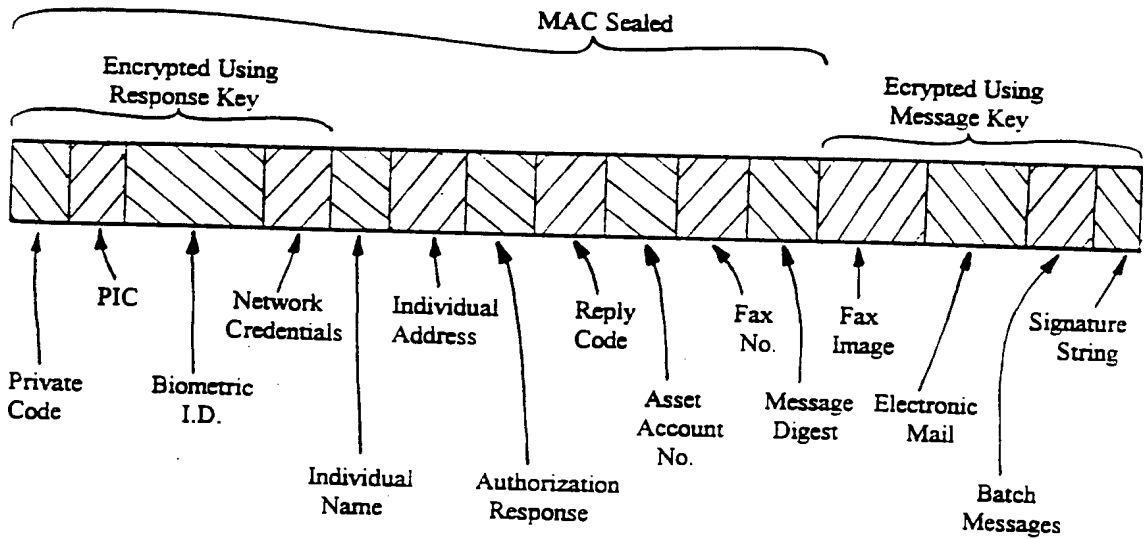


FIG. 6

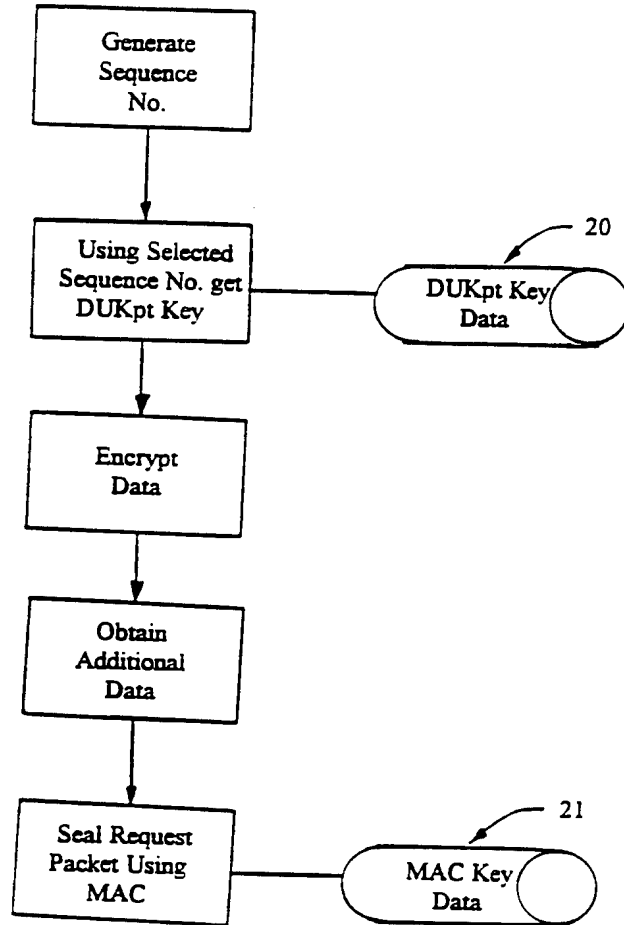


FIG. 7

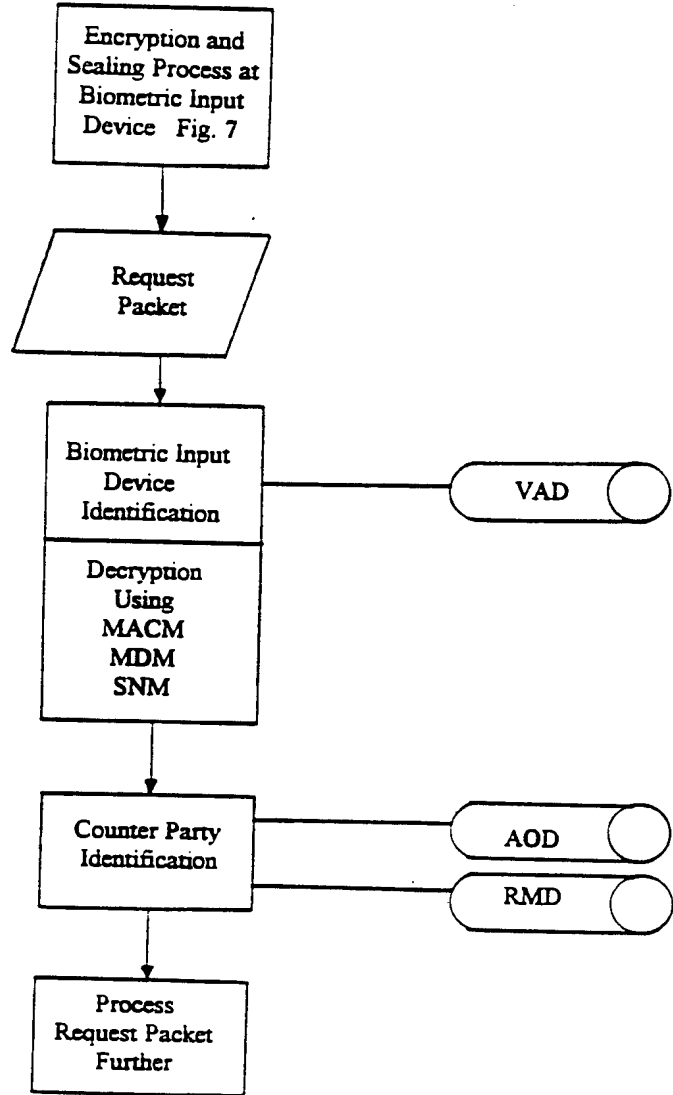


FIG. 8

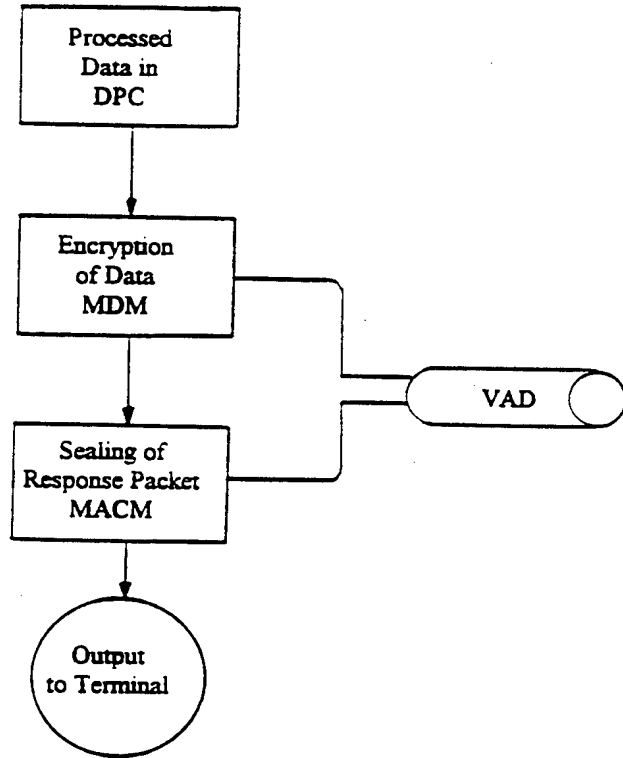


FIG. 9

9/20

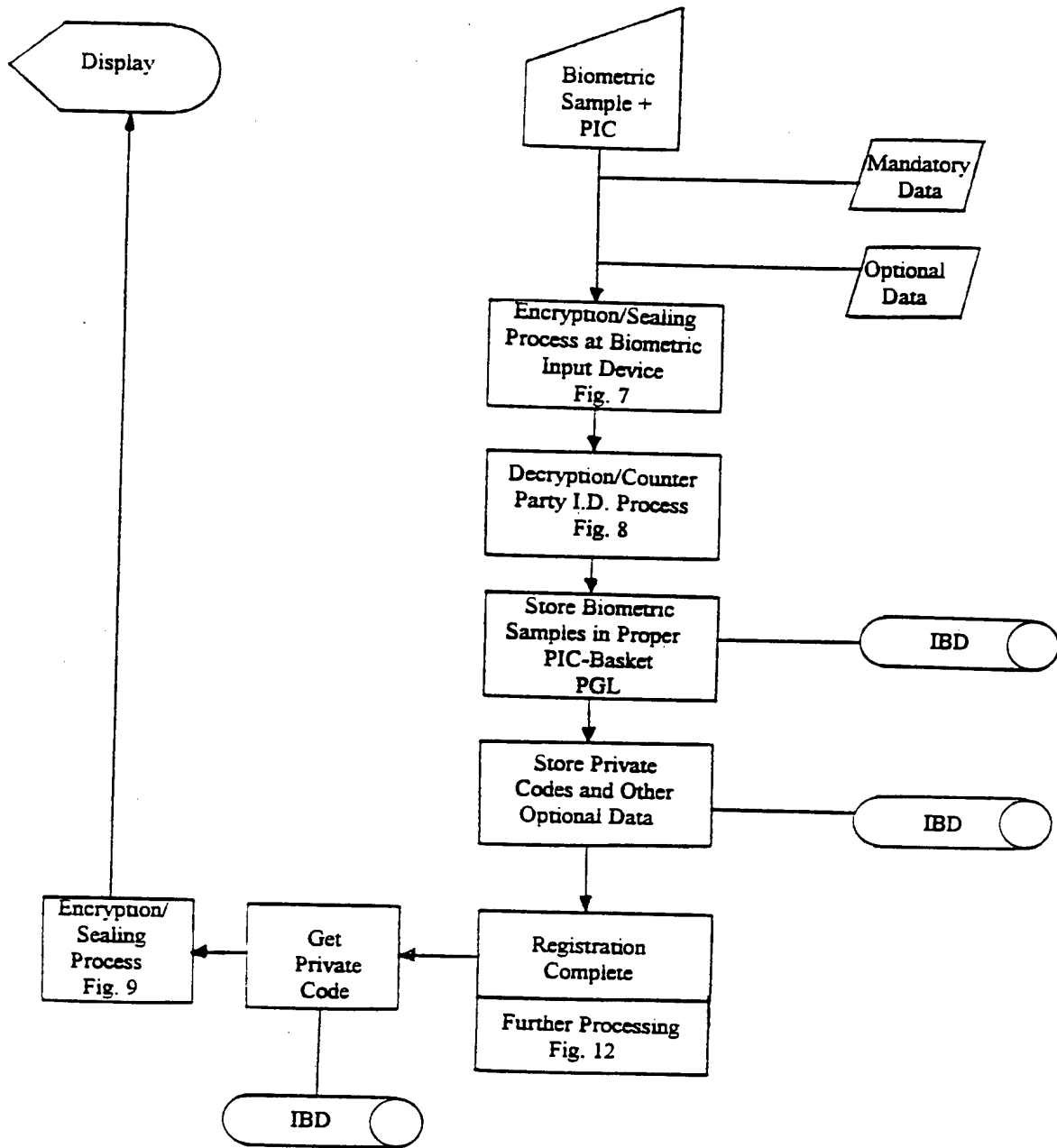


FIG. 10

10/20

PATENT

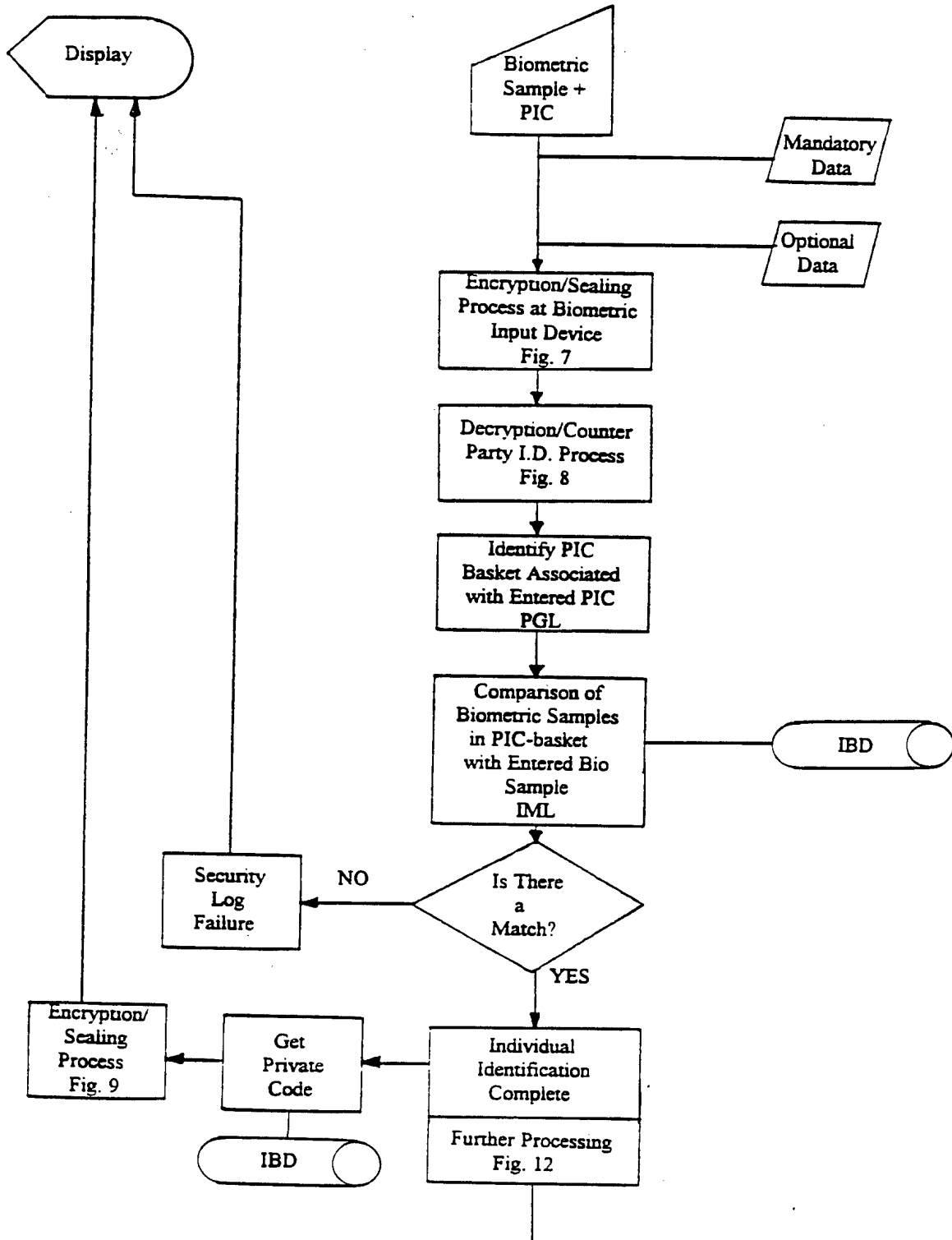


FIG. 11

11/20

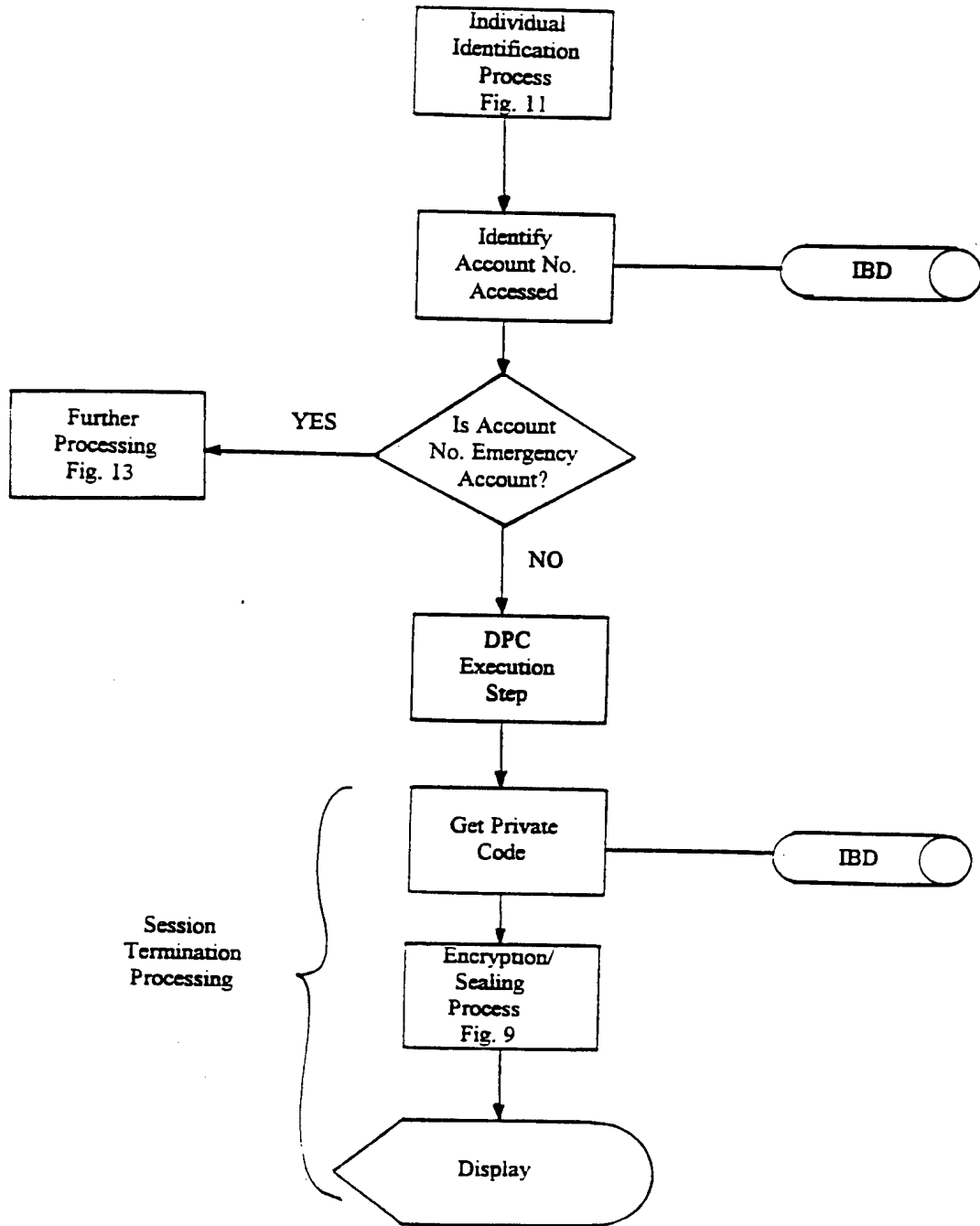


FIG. 12

12/20

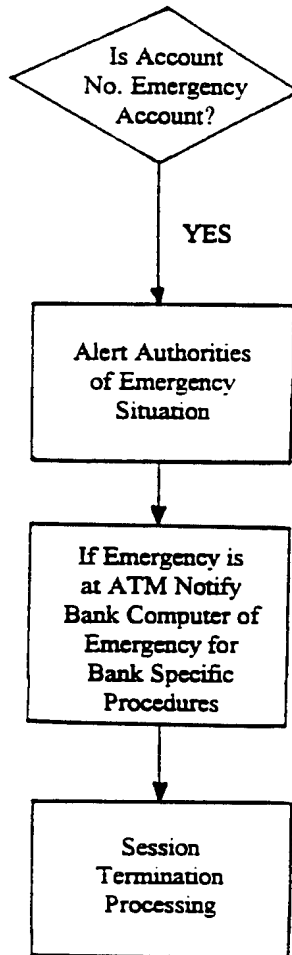


FIG. 13

13/20

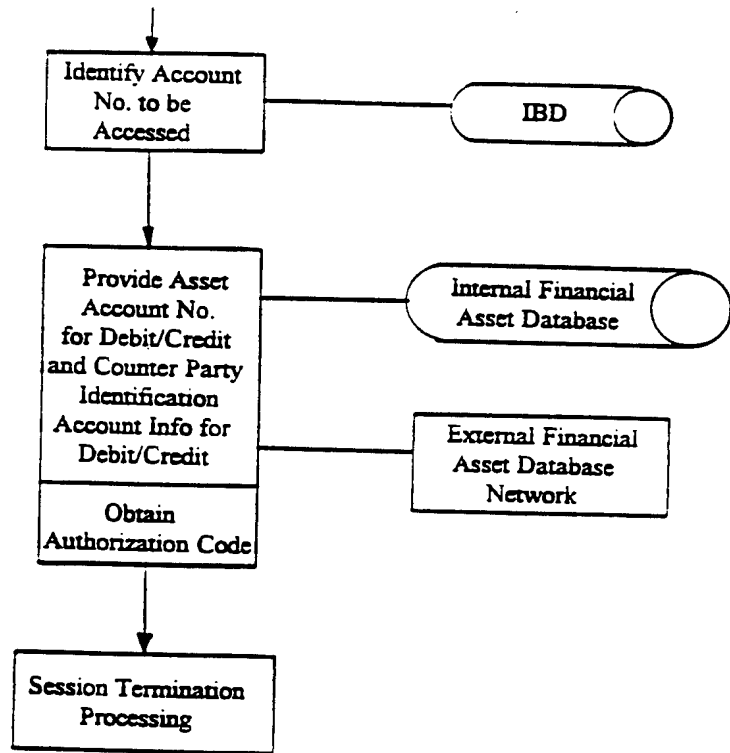


FIG. 14

14/20

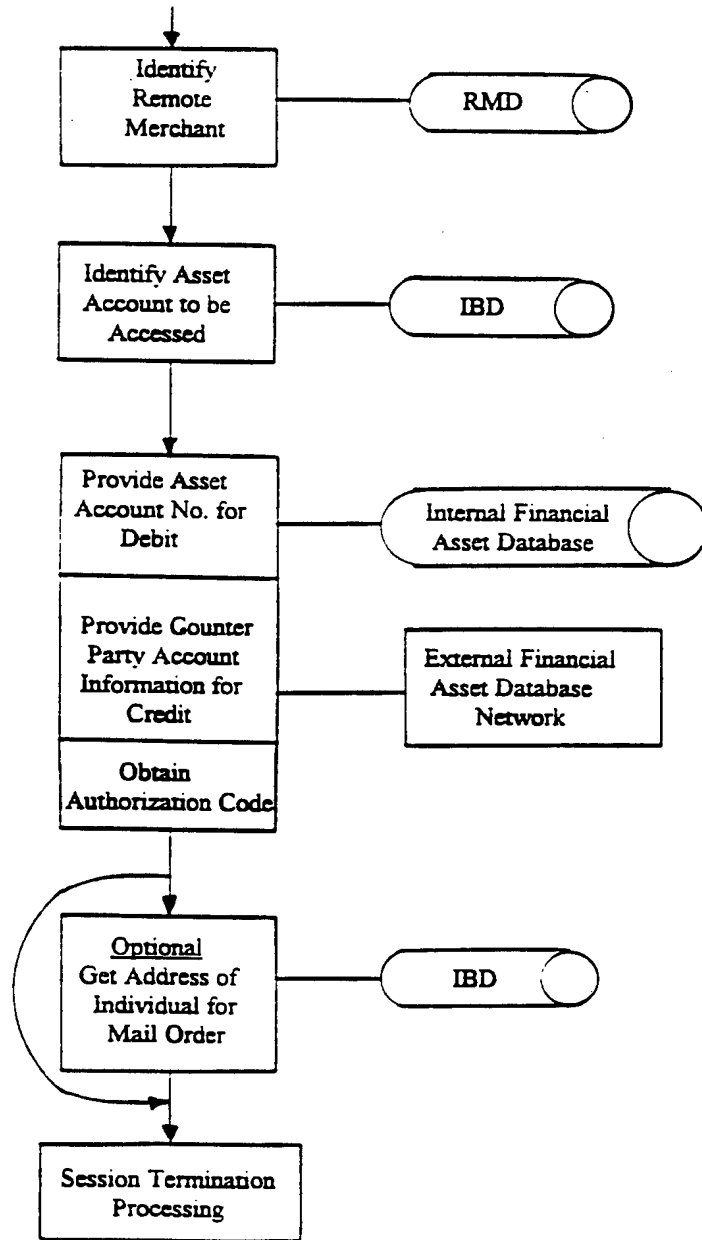


FIG. 15

15/20

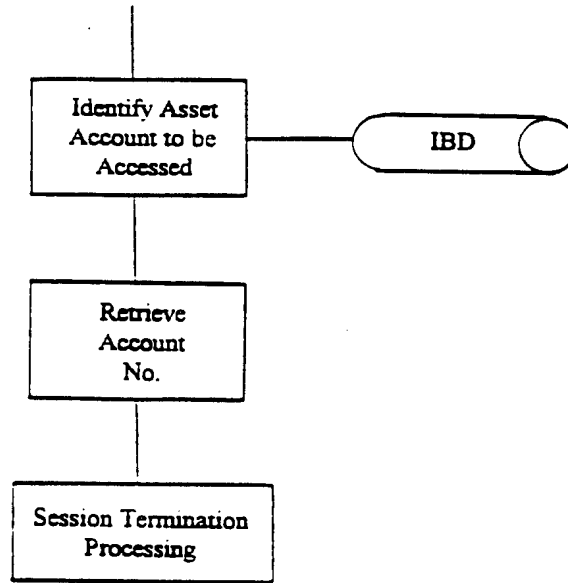


FIG. 16

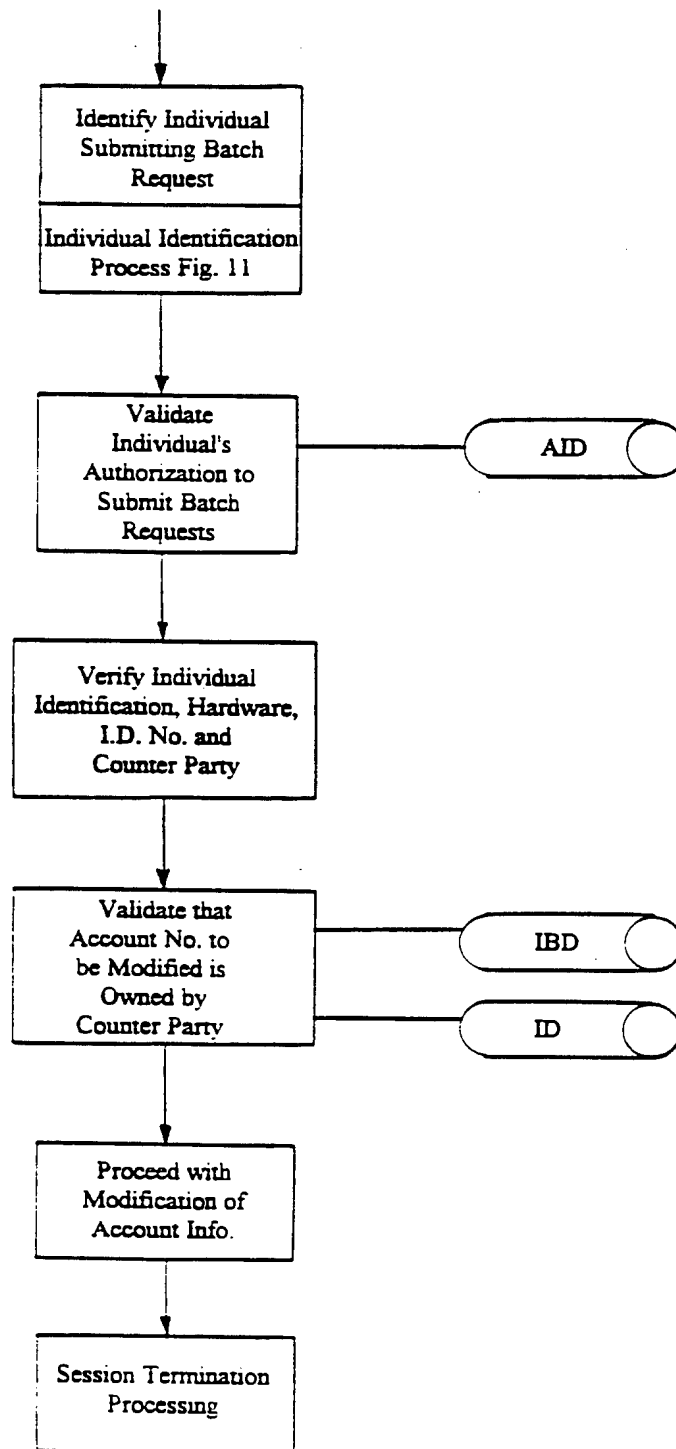


FIG. 17

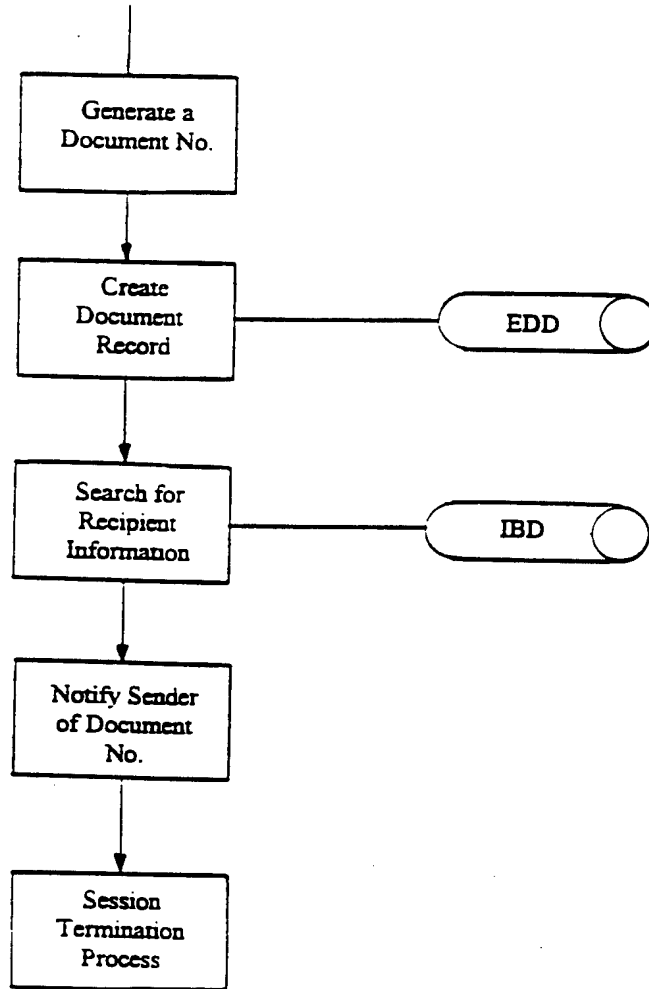


FIG. 18

18/20

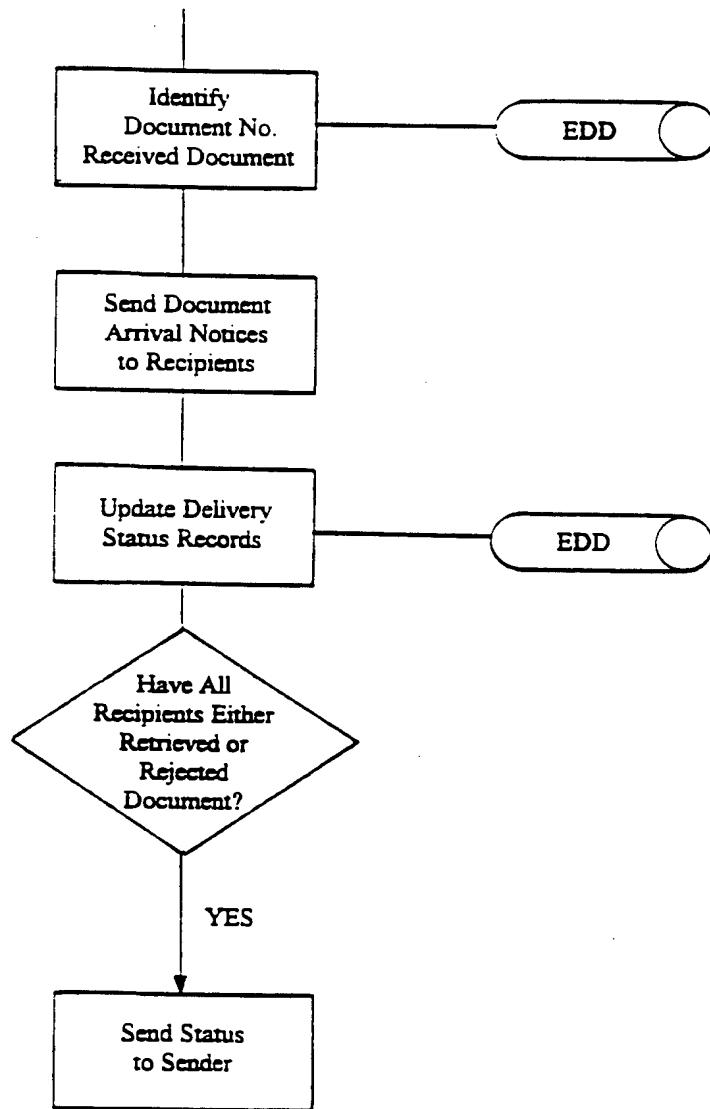


FIG. 19

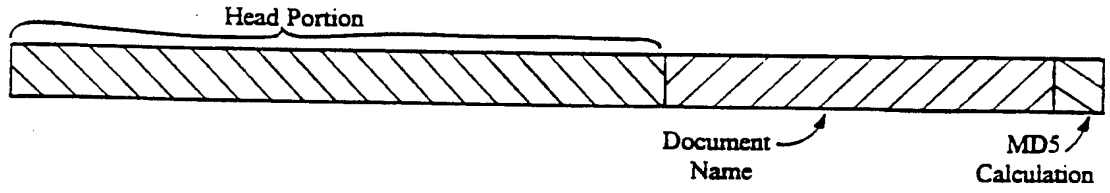


FIG. 20A

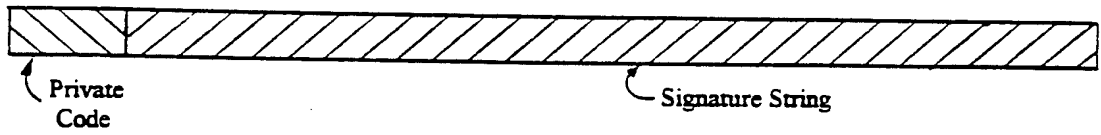


FIG. 20B

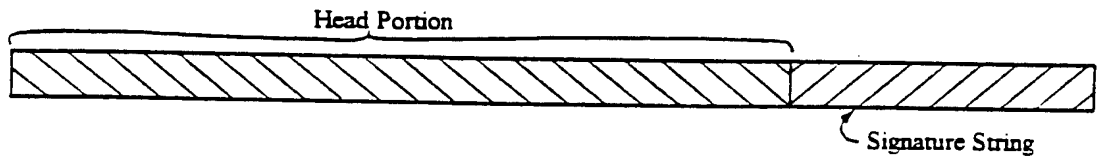


FIG. 20C

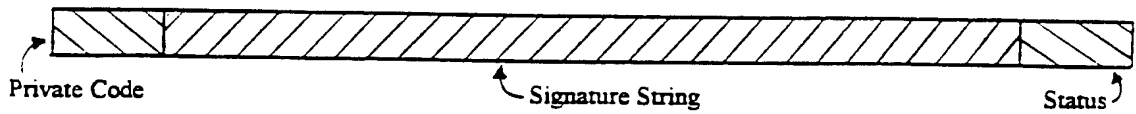


FIG. 20D

20/20

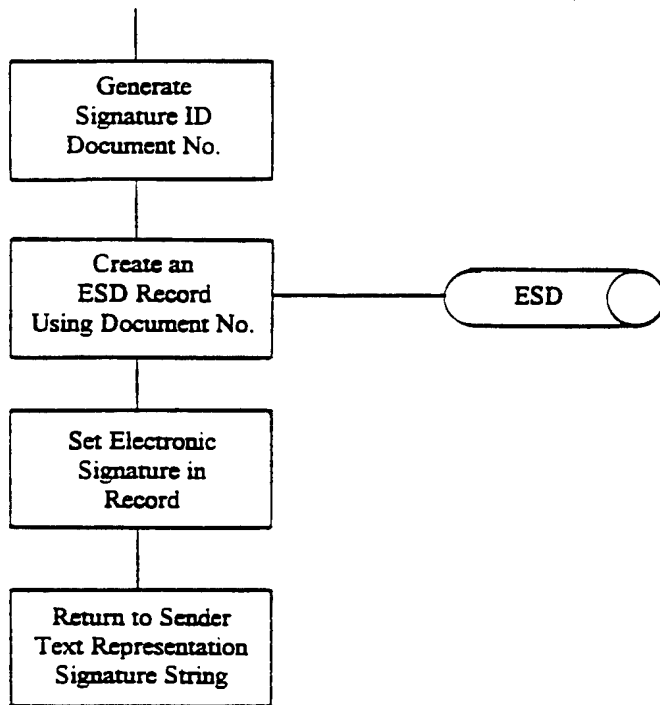


FIG. 21

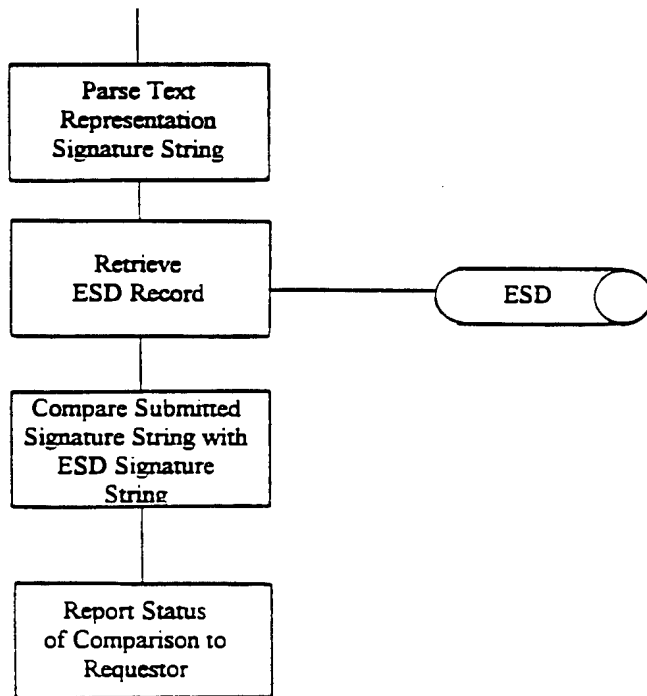


FIG. 22

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US96/07185

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :GO6K 9/00

US CL :Please See Extra Sheet.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 902/1, 2, 3, 4, 5, 6, 22, 26, 27, 31, 32, 33; 340/825.34; 235/380; 382/115

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US, A, 5,229,764 (MATCHETT ET AL) 20 July 1993, see abstract, figure 1, column 1, lines 6-59, column 8, lines 19-25.	1-87
Y	US, A, 5,191,611 (LANG) 02 March 1993, column 16, line 27.	1-87

Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents:	"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be part of particular relevance	"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document published on or after the international filing date	"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"g" document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means	
"P" document published prior to the international filing date but later than the priority date claimed	

Date of the actual completion of the international search 03 JULY 1996	Date of mailing of the international search report 26 AUG 1996
---	--

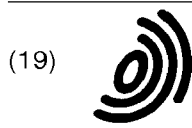
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer <i>Leo Boudreau</i> LEO BOUDREAU Telephone No. (703) 308-7595
---	---

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US96/07185

A. CLASSIFICATION OF SUBJECT MATTER:
US CL :

902/1, 2, 3, 4, 5, 6, 22, 26, 27, 31, 32, 33; 340/825.34; 235/380; 382/115



(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention
of the grant of the patent:
04.01.2006 Bulletin 2006/01

(51) Int Cl.:
H04L 9/32 (2006.01)

(21) Application number: **99112066.8**

(22) Date of filing: **22.06.1999**

(54) **Remote authentication system**

Vorrichtung zur entfernten Authentifikation

Système d'authentification à distance

(84) Designated Contracting States:
DE FR GB

(30) Priority: **11.09.1998 JP 25781398**

(43) Date of publication of application:
15.03.2000 Bulletin 2000/11

(73) Proprietor: **MITSUBISHI DENKI KABUSHIKI
KAISHA
Tokyo 100-8310 (JP)**

(72) Inventors:
• **Nakamura, Hiroshi,
c/o Mitsubishi Denki K.K.
Tokyo 100-8310 (JP)**

- **Fujii, Teruko,
c/o Mitsubishi Denki K.K.
Tokyo 100-8310 (JP)**
- **Sadakane, Tetsuo,
c/o Mitsubishi Denki K.K.
Tokyo 100-8310 (JP)**
- **Baba, Yoshimasa,
c/o Mitsubishi Denki K.K.
Tokyo 100-8310 (JP)**

(74) Representative: **Pfenning, Meinig & Partner GbR
Mozartstrasse 17
80336 München (DE)**

(56) References cited:
**WO-A-96/36934 WO-A-97/25800
DE-A- 4 443 339 US-A- 4 438 824
US-A- 5 280 527**

EP 0 986 209 B1

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

Description

BACKGROUND OF THE INVENTION

1. Field of the Invention

[0001] The present invention relates to a remote authentication system identifying a person with biometrics.

2. Description of the Related Art

[0002] Heretofore, so as to perform security protection in an information processing system connected to a network, it is necessary to identify a person and to judge approval or disapproval of access of the person, that is, to perform authentication. In addition, in cash dispensers of banks and the like, authentication for identifying a person and accessing the person's transaction information, and authentication for entrance into and exit from confidential research sites, membership clubs, and the like, which have high confidentiality, are performed.

[0003] Identification of a person and authorization of the person's qualification, that is, authentication is performed with a magnetic card, an IC card, which are positioned similarly to an identification card and the like, and the person's memory such as a password, and combination of them. There are problems, that the authentication cannot be performed because the password is forgotten, and the magnetic card and IC card are lost or broken, and another person, who is not the principal, is authenticated with masquerading by burglary and leakage of password information.

[0004] In addition, as one of means for authenticating a user over a network, there is a digital signature for indirectly authenticating the user by authenticating a message created by the user. In the digital signature, first, a message sender attaches a cryptogram that is encrypted from a message digest, into which an original message is compressed, with the sender's cryptographic key to the message. A message receiver confirms that the message is one, which the sender himself/herself sent, and that the message is not tampered, by creating a message digest from the message received, decoding the message digest from the cryptogram, which is attached, with the sender's decoding key, and confirming coincidence of these two message digests.

[0005] In addition, in the above-described encryption method, there are a common key encryption method, using the same key for a cryptographic key and a decoding key, and a public key encryption method using different keys for the cryptographic key and decoding key. In the public key encryption method, when one key is set as a secret key and is kept safely and another key is officially announced as a public key, the cryptogram encrypted with the public key cannot be decoded into the original message if a receiver has not the secret key, and hence the sender can transfer the message in such a form that only the receiver, who is desired by the sender, can de-

code, and the cryptogram encrypted with the secret key can be decoded with the public key into the original message, and hence the receiver can authenticate that the message is one from the sender herself/himself having the secret key.

[0006] Heretofore, although, in RFC1421 and RFC1422 (PEM: Privacy Enhancement for Internet Electronic Mail) that are registered in RFC (Request For Comment) of IETF (Internet Engineering Task Force), the digital signature and message encryption are performed with the public key encryption method and common key encryption method, there is a problem that it is necessary to administrate the secret key on the sender's hands since the sender uses the own secret key, for example, to safely keep the secret key with saving the secret key in a floppy disk, a magnetic card, and an IC card.

[0007] On the other hand, in the authentication with biometrics information, which is a person's biological characteristic such as finger print information, palm print information, handwriting information, and retina information, it is difficult to perform masquerade and is unnecessary to administrate the information of the secret key so long as the user himself/herself presents, and it is possible to resolve the complexness of keeping a baggage and the threat of loss at the time of the authentication of a person and the complexness of memory at the time of the authentication of a password with the magnetic card and IC card. Nevertheless, there are problems that, if the authentication with the biometrics information is necessary in a wide range, the equipment for performing the centralized administration and authentication of the biometrics information is necessary, and that it is necessary to keep security with concealing the user's biometrics information at the time of transferring the biometrics information to the equipment, performing the authentication, from the viewpoint of protection of privacy.

[0008] Furthermore, in general, random numbers are used for creating a cryptographic key in a system creating the cryptographic key used for concealing the biometrics information. Nevertheless, there is also a problem that it is important to eliminate the tendency of the random numbers so as to make it difficult to break the cryptographic key.

[0009] In addition, an apparatus acquiring biometrics should be properly administrated from the viewpoint of protection of users' privacy, and it is necessary to authenticate an administrator. Nevertheless, there is a problem that, since another person cannot act for the administrator if the authentication of this administrator was performed with biometrics, another person can never perform the access to the biometrics acquisition apparatus including initialization. Furthermore, there is a problem that even a valid administrator can never perform the access to the biometrics acquisition apparatus including initialization if the biometrics used for the authentication is largely changed or lost by suffering damage in an accident in case of the valid administrator.

[0010] Moreover, in general, a system performing user

authentication is required to early find an invalid authentication, for example, as for a cash card in a bank, there is means for making a cash card unusable if authentication with a preset number of times of password inputs is unsuccessful. Also, a user authentication system with the biometrics is required to early find an invalid authentication. Nevertheless, a condition of biometrics is different every person, for example, in a system authenticating a person with finger print matching, a minimum matching rate identifying a person as the principal is determined, but a person whose finger is rough or worn gets a low matching rate even if the person can obtain the best biometrics information at that time, and a failure probability of the authentication itself increase if the matching rate decreases due to a minor failure such as insufficient contact at the time of acquiring the finger print. Therefore there is a problem that it cannot be equally performed for all the persons that it is judged to be an unsuccessful authentication within only the preset number of times.

[0011] WO 96/36934 describes a tokenless identification system and method which are principally based on a correlative comparison of a unique biometric sample, such as a finger print or voice recording, gathered directly from a person of an unknown user, with an authenticated biometric sample of the same type obtained and stored previously. A biometric acquisition apparatus acquires a public key from public key partners or holders of the RSA public key patent. The data processing center decodes with a message decrypt module and provides the derived unique key per transaction (DUKPT). This key is used to create the digital encryption standard (DES) which is the key of the common key method.

SUMMARY OF THE INVENTION

[0012] The present invention is to solve above problems, and an object of the present invention is to provide a remote authentication system which securely authenticates with protecting biometrics information, which is user's personal information, and is firm on security when performing authentication of a person with the biometrics information, and a remote authentication method.

[0013] This object is realized by the features of claim 1.

[0014] Advantageous aspects are given by the features of the subclaims.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015]

Fig. 1 is a block diagram showing the configuration of a first embodiment of an Web system where a remote authentication system according to the present invention is applied;

Fig. 2 is a timing chart for explaining the processing of authentication in the Web system in Fig. 1;

Fig. 3 is a block diagram showing the configuration of a second embodiment of a database retrieval sys-

tem where a remote authentication system according to the present invention is applied;

Fig. 4 is a timing chart for explaining the processing of authentication in the database retrieval system in Fig. 3;

Fig. 5 is a block diagram showing the configuration of a third embodiment of an Web system where a remote authentication system according to the present invention is applied;

Fig. 6 is a timing chart for explaining the processing of authentication in the Web system in Fig. 5;

Fig. 7 is a block diagram showing the configuration of a fourth embodiment at the time of administration of a finger print acquisition apparatus where a remote authentication system according to the present invention is applied;

Fig. 8 is a block diagram showing the configuration of a fifth embodiment of an authentication server where a remote authentication system according to the present invention is applied.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0016] Hereinafter, embodiments of the present invention will be described with reference to drawings.

Embodiment 1.

[0017] Fig. 1 shows the configuration of a Web system being designed as authentication system where the present invention is applied. Over a network 1, an authentication server 3, a computer system being designed as Web server 4, and a user terminal 5 are connected, and a biometrics acquisition apparatus 6 is connected to the user terminal 5. In this authentication system, if a user accesses the Web server 4, through the user terminal 5, the Web server 4 receives user's personal authentication from the authentication server 3, and according to the result, the Web server 4 performs access control to the user.

[0018] The authentication server 3 is a computer system namely a system having a CPU, memory, a disk, communication control, and the like) such as a personal computer and a workstation that are composed of an authentication controller 3A, an encryption processing unit 3C, and an authentication information database 3B, and announces one key in a public key method as a public key and conceals another key as a secret key.

[0019] In addition, the Web server 4 is a computer system such as a personal computer and a workstation where a Web server database 4A, an encryption processing unit 4D, an authentication request unit 4B, and an application of a Web server software 4C (hereinafter, software is written as S/W) that is an application requiring personal authentication operate.

[0020] In addition, the user terminal 5 is a computer system such as a personal computer and a workstation where a browser 5A displaying information of the Web

server terminal 4, and authentication information acquisition S/W 5B operate. Furthermore, a biometrics acquisition apparatus 6 is connected to the user terminal 5. The biometrics acquisition apparatus 6 represents a finger print acquisition apparatus 7 and a palm print acquisition apparatus 8 that acquire finger print of a human body and palm print information with image processing as biometrics information, a character recognition tablet 9 acquiring handwriting information, which a user draws, as biometrics information, a retina acquisition apparatus 10 acquiring retina information of a human body as the biometrics information with eyeground (fundus) scanning and the like, and the like.

[0021] Here, a case that the finger print acquisition apparatus 7 is used as the biometrics acquisition apparatus 6 will be described as an example. In addition, the biometrics information acquired by the biometrics acquisition apparatus 6 such as the finger print acquisition apparatus 7 can be image data, image data that is not processed such as electrostatic data, and characteristic point data obtained by extracting characteristics from image data. The finger print acquisition apparatus 7 is composed of a finger print information acquisition unit 7A acquiring finger print information with image processing and the like and transferring the finger print information to the user terminal, an encryption processing unit 7B encrypting the finger print information, and a public key acquisition unit 7C acquiring a public key of the authentication server 3.

[0022] Next, operation will be described.

[0023] A flow of authentication processing in the authentication system like this is shown in Fig. 2.

[0024] First, a case (SP5) that a user accesses information in the Web server database 4A, which has high confidentiality, in the Web server 4 with the browser 5A that is an application operating in the user terminal 5 will be described. The Web server S/W 4C, which is an application performing access control of the information having high confidentiality, is required to perform the user authentication so as to judge whether the user has an access authority.

[0025] The authentication information acquisition S/W 5B in the user terminal 5 acquires the finger print information, which is biometrics information necessary for the authentication, from the finger print acquisition apparatus 7 (SP6). At this time, the S/W 5B may operate with cooperating with other S/W (software such as a driver acquiring the authentication information).

[0026] The finger print information acquisition unit 7A in the finger print acquisition apparatus 7, which is instructed to acquire the finger print information by the authentication information acquisition S/W 5B in the user terminal 5, acquires the finger print information from the user (SP1). Although the encryption processing unit 7B encrypts this finger print information since this finger print information is user's inherent personal information, first, the encryption processing unit 7B creates a common key in the common key method for encrypting this finger print

information, and encrypts the finger print information with this common key. At the same time, the encryption processing unit 7B acquires date and time information, creates a message digest with connecting the date and time information with the common key, and further encrypts the message digest with the common key (SP2).

[0027] The public key acquisition unit 7C in the finger print acquisition apparatus 7 acquires a public key of the authentication server from user's instruction such as a floppy disk, a magnetic card, an IC card, or key entry. Alternatively, if the finger print acquisition apparatus 7 is properly administrated, the public key of the authentication server 3 is fixedly saved in the public key acquisition unit 7C in the finger print acquisition apparatus 7, and hence the user may use the public key after recognizing the public key. Next, the encryption processing unit 7B encrypts the common key with the public key of the authentication server 3 (SP3).

[0028] Then, the finger print acquisition unit 7A transfers the finger print information encrypted, the date and time information, the message digest containing the date and time information with the common key that is encrypted, and the encrypted common key as the authentication information to the authentication information acquisition S/W 5B in the user terminal 5 (SP4).

[0029] The authentication information acquisition S/W 5B in the user terminal 5 transfers the authentication information, which is acquired, to the Web server 4 through the browser 5A. At this time, the browser 5A transfers the authentication information with adding a user ID such as a user name and a mail address, which the browser 5A acquires separately (SP7).

[0030] The authentication request unit 4B in the Web server 4 transfers the authentication information, which the authentication request unit 4B acquires through the Web server S/W 4C, to the authentication controller 3A in the authentication server 3 (SP9).

[0031] The authentication controller 3A in the authentication server 3 makes the encryption processing unit 3C decode the authentication information transferred, and performs the user authentication. At this time, the encryption processing unit 3C compares the message digest created from the date and time information and common key, which are transferred, in the authentication server 3 with the message digest decoded from the message digest created with connecting the date and time information, which is encrypted, with the common key, and confirms the validity of the date and time, when the authentication information was created, in consideration of transfer delay (SP12).

[0032] The authentication controller 3A performs finger print matching from the finger print information and user ID, which are included in the authentication information transferred, and personal information originally saved in the authentication information database 3B in the authentication server 3. The authentication controller 3A creates the result of the authentication showing that the user is valid if the authentication controller 3A iden-

ifies the user as the principal in consequence of matching, or judges that the user is not the principal if the authentication controller 3A cannot identify the user as the principal in consequence of the matching, and creates the result of the authentication. This result of the authentication is delivered to the encryption processing unit 3C, and the encryption processing unit 3C creates a message digest of the result of the authentication, encrypts the message digest with the secret key of the authentication server 3, that is, performs digital signature, and delivers this message digest, which is encrypted, to the authentication controller 3A. The authentication controller 3A informs the authentication request unit 4B in the Web server 4 of the result of the authentication with including the message digest, which is encrypted, in the result of the authentication (SP13).

[0033] The authentication request unit 4B in the Web server 4 that receiving the result of the authentication informs the encryption processing unit 4D of the result of the authentication. The encryption processing unit 4D decodes the informed message digest, which is encrypted, with the public key of the authentication server 3, and confirms that the message digest is surely the valid message from the authentication server 3 by comparing the decoded message digest with the message digest of the informed result of the authentication (SP10). If the authentication request unit 4B is informed from the encryption processing unit 4D that the information was the valid information from the authentication server 3, the authentication request unit 4B informs the Web server S/W 4C of the result of the authentication. The Web server S/W 4C judges approval or disapproval of access to the information in the Web server database, which has high confidentiality, to the user according to the result of the authentication (SP11). For example, the Web server S/W 4C performs operation to the user access such as the display of the confidential information.

[0034] In this manner, the finger print information that is user's personal information is encrypted with the common key created, the common key is encrypted with the public key of the authentication server 3, which the user set, and the public key of the authentication server 3 is directly set by the user in the finger print acquisition apparatus 7. Hence, there is such an effect that it is possible to securely protect the user's personal privacy, which is the finger print information that is the biometrics information, in a style of reflecting user's intention since the finger print information is transferred over the network in such a condition that only the authentication server 3, which the user assigned, can decode the finger print information. Furthermore, a user can instruct only a public key of the authentication server 3 with a floppy disk, a magnetic card, an IC card, or key entry to the finger print acquisition apparatus 7, there is no problem on security even if the floppy disk, magnetic card, or IC card is lost or stolen, which saves this public key, and the user can receive the personal authentication with a substitute,

which saves the same public key or the same article. There is another effect that it is unnecessary to perform processing such as special notification and reissue at the time of loss and burglar and it is possible to lighten the administration load.

[0035] In addition, since the data and time, when the authentication information was created, is confirmed in the authentication server 3, it is possible to prevent reuse of the invalid authentication information, and to keep security high since it can be confirmed in the Web server 4 in the authentication-requester's side whether the authentication is performed by the authentication information authentication server 3.

[0036] Although the present invention is applied in the authentication system in this embodiment, the same effect can be obtained even if the Web server S/W 4C and browser 5A are other applications, constructing another system, such as accounting information administration server S/W and accounting information administration client S/W, and database retrieval server S/W and database retrieval client S/W.

Embodiment 2.

[0037] This embodiment is obtained by simplifying the first embodiment, and the Web server 4 and user terminal 5 in Fig. 1 become only a user terminals 5 in Fig. 3. Since, in Fig. 3 where the same symbols are assigned to the parts corresponding to the parts in Fig. 1, applications for which the personal authentication is necessary present in only the user terminal 5, the Web server S/W 4C and two applications, constructing the browser 5A, that are shown in Fig. 1 are replaced to database retrieval S/W 5E, and the Web server database 4A is replaced to a local database 5C. In this case, the authentication request unit 4B and encryption processing unit 4D that construct the Web server 4 in Fig. 1 become a component of the user terminal 5 in Fig. 3.

[0038] In the second embodiment, the user terminal 5 is a computer system such as a personal computer and a workstation, where the local database 5C, an encryption processing unit 5F, a authentication request unit 5D, a database retrieval S/W 5E that is an application for which the personal authentication is required, and authentication information acquisition S/W 5B operate. In addition, a biometrics acquisition apparatus 6 is connected to the user terminal 5, and has the same configuration as that in the first embodiment. Furthermore, the authentication server 3 also has the same configuration as that in the first embodiment described above.

[0039] Here, a case that a finger print acquisition apparatus 7 is used as the biometrics acquisition apparatus 6 will be exemplified.

[0040] Next, operation will be described.

[0041] Fundamentally, this is similar to that in the first embodiment, and in Fig. 4 where the same symbols are assigned to the parts corresponding to those in Fig. 2, first, a case that a user accesses information in the local

database 5C, which has high confidentiality, with the database retrieval S/W 5E that is an application operating in the user terminal 5 will be described. The database retrieval S/W 5E that is an application performing access control of the information having high confidentiality is required to perform the user authentication so as to judge whether the user has access authorization (SP5).

[0042] The authentication information acquisition S/W 5B in the user terminal 5 acquires the finger print information, which is necessary for the authentication, from the finger print information acquisition apparatus 7 (SP6). At this time, this S/W 5B may cooperate with other S/W (software such as a driver acquiring the authentication information).

[0043] The authentication information acquisition unit 7A in the finger print acquisition apparatus, which is instructed to acquire the finger print information from the authentication information acquisition S/W 5B in the user terminal 5 acquires the finger print information from the user (SP1). Although encryption processing unit 7B encrypts this finger print information since this finger print information is user's personal information, first, the encryption processing unit 7B creates a common key in the common key encryption method for encrypting this finger print information, and encrypts the finger print information with this common key. At the same time, the encryption processing unit 7B acquires date and time information, creates a message digest with connecting the date and time information with the common key, and further encrypts the message digest with the common key (SP2).

[0044] The public key acquisition unit 7C in the finger print acquisition apparatus 7 acquires the public key of the authentication server 3 from user's instruction such as a floppy disk, a magnetic card, an IC card, or key entry. Alternatively, if the finger print acquisition apparatus 7 is properly administrated, the public key of the authentication server 3 is fixedly saved in the public key acquisition unit 7C in the finger print acquisition apparatus 7, and hence the user may use the public key after recognizing the public key. Next, the encryption processing unit 7B encrypts the common key with the public key of the authentication server 3 (SP3). Then, the finger print acquisition unit 7A transfers the finger print information encrypted, the date and time information, the message digest with connecting the date and time information with the common key that is encrypted, and the encrypted common key as the authentication information to the authentication information acquisition S/W 5B in the user terminal 5 (SP4).

[0045] The authentication information acquisition S/W 5B in the user terminal 5 acquires a user ID such as a user name and a mail and adds them to the authentication information (SP7).

[0046] The authentication request unit 5D transfers this authentication information to the authentication controller 3A in the authentication server 3 (SP7).

[0047] The authentication controller 3A in the authentication server 3 makes the encryption processing unit

3C decode the authentication information transferred, and performs the user authentication. At this time, the encryption processing unit 3C compares the message digest created from the date and time information and common key, which is transferred, in the authentication server 3 with the message digest decoded from the message digest obtained by connecting the date and time information, which is encrypted, with the common key, and confirms the validity of the date and time, when the authentication information was created, in consideration of transfer delay (SP12).

[0048] The authentication controller 3A performs finger print matching from the finger print information and user ID, which are included in the authentication information transferred, and personal information originally saved in the authentication information database 3B in the authentication server 3. The authentication controller 3A creates the result of the authentication showing that the user is valid if the authentication controller 3A identifies the user as the principal in consequence of matching, or judges that the user is not the principal if the authentication controller 3A cannot identify the user as the principal in consequence of the matching, and creates the result of the authentication. This result of the authentication is delivered to the encryption processing unit 3C, and the encryption processing unit 3C creates a message digest of the result of the authentication, encrypts the message digest with the secret key of the authentication server 3, that is, performs digital signature, and delivers this message digest, which is encrypted, to the authentication controller 3A. The authentication controller 3A informs the authentication request unit 5D in the user terminal 5 of the result of the authentication with including the message digest, which is encrypted, in the result of the authentication (SP13).

[0049] The authentication request unit 5D in the user terminal 5 that receiving the result of the authentication informs the encryption processing unit 5F of the result of the authentication. The encryption processing unit 5F decodes the informed message digest, which is encrypted, with the public key of the authentication server 3, and confirms that the message digest is surely the valid message from the authentication server 3 by comparing the decoded message digest with the message digest of the informed result of the authentication (SP10). If the authentication request unit 5D receives from the encryption processing unit 5D the result of confirmation that the information is the valid information from the authentication server 3, the authentication request unit 5D informs the database retrieval S/W 5E of the result of the authentication. The database retrieval S/W 5E judges approval or disapproval of access to the information in the local database 5C, which has high confidentiality, to the user according to the result of the authentication. For example, the database retrieval S/W 5E performs operation to, the user access such as the display of the confidential information (SP11).

[0050] According to this configuration, when the user

terminal 5 requests the authentication server 3 to perform the personal authentication, it is possible to obtain the same effects as those in the first embodiment.

[0051] Although the present invention is applied in a database retrieval system in this embodiment, the same effects can be obtained even if the database retrieval S/W is an application, constructing another system, such as accounting information administration S/W.

Embodiment 3.

[0052] This third embodiment is an embodiment where the encryption processing unit 7B and public key acquisition unit 7C in the finger print acquisition apparatus 7 that is a biometrics acquisition apparatus 6 in the first embodiment present in the user terminal 5.

[0053] In Fig. 5 where the same symbols are assigned to the parts corresponding to those in Fig. 1, the user terminal 5 is a computer system such as a personal computer and a workstation, where a browser 5A displaying the information of the Web server terminal 4, an encryption processing unit 5F encrypting the finger print information, a public key acquisition unit 5G acquiring the public key of the authentication server 3, and an authentication information acquisition S/W 5B operate. In addition, a biometrics acquisition apparatus 6 is connected to the user terminal 5. Furthermore, the authentication server 3 and Web server 4 have the same configuration as that in the first embodiment.

[0054] In addition, the biometrics information which the biometrics acquisition apparatus 6 in this embodiment acquires can be image data, image data that is not processed such as electrostatic data, and also characteristic point data obtained by extracting characteristics from image data. The biometrics acquisition apparatus 6 can be a simple device that only acquires image data and does not have a CPU. Here, a case that the finger print acquisition apparatus 7 is used as the biometrics acquisition apparatus 6 will be exemplified.

[0055] The finger print acquisition apparatus 7 is composed of a finger print information acquisition unit 7A that acquires the finger print information by performing image processing and the like and transfers the finger print information to the user terminal.

[0056] Next, operation will be described.

[0057] Fundamentally, the operation is the same as that in the first embodiment, in Fig. 6 where the same symbols are assigned to the parts corresponding to those in Fig. 2, first, a case that a user accesses the information in the Web server database 4A, which has high confidentiality, in the Web server 4 with the browser 5A that is an application operating in the user terminal 5 will be described (SP5). The Web server S/W 4C, which is an application performing access control of the information having high confidentiality, is required to perform the user authentication so as to judge whether the user has an access authority.

[0058] The authentication information acquisition S/W

5B in the user terminal 5 acquires the finger print information, which is biometrics information necessary for the authentication, from the finger print acquisition apparatus 7 (SP6). At this time, the S/W 4C may operate with co-operating with other S/W (software such as a driver acquiring the authentication information).

[0059] The finger print information acquisition unit 7A in the finger print acquisition apparatus 7 which is instructed to acquire the finger print information by the authentication information acquisition S/W 5B in the user terminal 5 acquires the finger print information from the user (SP1), and transfers the finger print information to the authentication information acquisition S/W 5B in the user terminal 5 (Sp4).

[0060] The authentication information acquisition S/W 5B in the user terminal 5 makes the encryption processing unit 5F encrypt this finger print information since this finger print information is user's inherent personal information. First, the encryption processing unit 5F creates a common key in the common key method for encrypting this finger print information, and encrypts the finger print information with this common key. At the same time, the encryption processing unit 5F acquires date and time information, creates a message digest with connecting the date and time information with the common key, and further encrypts the message digest with the common key (SP2).

[0061] The public key acquisition unit 5G in the user terminal 5 acquires a public key of the authentication server from user's instruction such as a floppy disk, a magnetic card, an IC card, or key entry.

[0062] Next, the encryption processing unit 5F encrypts the common key with the public key of the authentication server 3 (SP3). Then, the authentication information acquisition S/W 5B transfers the finger print information encrypted, the date and time information, the message digest with connecting the date and time information with the common key that is encrypted, and the encrypted common key, the acquired authentication information as the authentication information to the Web server 4 through the browser 5A. At this time, the browser 5A transfers the authentication information with adding a user ID such as a user name and a mail address, which the browser 5A acquires separately, to the authentication information (SP7).

[0063] The authentication request unit 4B in the Web server 4 transfers the authentication information, which the authentication request unit 4B acquires, to the authentication controller 3A in the authentication server 3 through the Web server S/W 4C (SP9).

[0064] The authentication controller 3A in the authentication server 3 makes the encryption processing unit 3C decode the authentication information transferred, and performs the user authentication. At this time, the encryption processing unit 3C compares the message digest created from the date and time information and common key, which are transferred, in the authentication server 3 with the message digest decoded from the mes-

sage digest obtained by connecting the date and time information, which is encrypted, with the common key, and confirms the validity of the date and time, when the authentication information was created, in consideration of transfer delay (SP12).

[0065] The authentication controller 3A performs finger print matching from the finger print information and user ID, which are included in the authentication information transferred, and personal information originally saved in the authentication information database 3B in the authentication server 3. The authentication controller 3A creates the result of the authentication showing that the user is valid if the authentication controller 3A identifies the user as the principal in consequence of matching, or judges that the user is not the principal if the authentication controller 3A cannot identify the user as the principal in consequence of the matching, and creates the result of the authentication. The result of this authentication is delivered to the encryption processing unit 3C, and the encryption processing unit 3C creates a message digest of the result of the authentication, encrypts the message digest with the secret key of the authentication server 3, that is, performs digital signature, and delivers this message digest, which is encrypted, to the authentication controller 3A. The authentication controller 3A informs the authentication request unit 4B in the Web server 4 of the result of the authentication with including the message digest, which is encrypted, in the result of the authentication (SP13).

[0066] The authentication request unit 4B in the Web server 4 receiving the result of the authentication informs the encryption processing unit 4D of the result of the authentication. The encryption processing unit 4D decodes the informed message digest, which is encrypted, with the public key of the authentication server 3, and confirms that the message digest is surely the valid message from the authentication server 3 by comparing the decoded message digest with the message digest of the informed result of the authentication (SP10). If the authentication request unit 4B is informed from the encryption processing unit 5D that it was confirmed that the information was the valid information from the authentication server 3, the authentication request unit 4B informs the Web server S/W 4C of the result of the authentication. The Web server S/W 4C judges approval or disapproval of access to the information in the Web server database 4A, which has high confidentiality, to the user according to the result of the authentication. For example, the Web server S/W 4C performs operation to the user access such as the display of the confidential information (SP11).

[0067] In this manner, the finger print information that is user's personal information is encrypted with the common key created, the common key is encrypted with the public key of the authentication server 3, which the user set, and the public key of the authentication server 3 is directly set by the user in the user terminal 5. Hence, there is such an effect that it is possible to securely protect the user's personal privacy, which is the finger print in-

formation that is the biometrics information, in a style of reflecting user's intention since the finger print information is transferred over the network in such a condition that only the authentication server 3, which the user assigned, can decode the finger print information. Nevertheless, although security becomes low in comparison with a case that the finger print information is encrypted from the finger print acquisition apparatus 7 since there arises a period, when the finger print information exists in the user terminal 5 without being encrypted, there is no problem if the user terminal 5 itself is properly administered, and there is an effect that the configuration of the finger print acquisition apparatus 7 becomes simple since the encryption processing unit and public key acquisition unit are unnecessary in the finger print acquisition apparatus 7. As effects except the above-described effects, the similar effects as those in the first embodiment can be obtained. In addition, this embodiment can be applied also to the application such as the database retrieval S/W 5E, which are shown in the second embodiment, and hence it is possible to obtain the same effects.

[0068] Furthermore, in all of the first, second, and third embodiments, a common key for encrypting the user's biometrics information obtained is created. Nevertheless, it is necessary to eliminate the tendency of the random numbers for creating the common key so as to make it difficult to break the common key. Since the biometrics information generally has values different every acquisition, the message digest of the biometrics information acquired is used as a part or all of the random numbers.

[0069] As described above, it is simply performed to eliminate the tendency of the generated random numbers since the random numbers generated from the message digest of the biometrics information acquired are generated. Furthermore, since a part or all of this random numbers are used as the random numbers for generating the common key, it is possible to generate the random numbers irrelevant to the number of authentication times and the time and to construct a system that is strong on security against the decoding of the common key.

Embodiment 4.

[0070] Although only the valid administrator can perform the administration of the biometrics information acquisition apparatus, it is necessary that the administrator, being not authenticated, or another person acting for the administrator can perform initialization of a biometrics acquisition apparatus if there arises such a state that no one cannot authenticate the valid administrator. This case will be described with exemplifying such a case that, in the finger print acquisition apparatus in the first and second embodiments, the finger print acquisition apparatus is properly administered and a public key of an authentication server is fixedly determined in the finger print acquisition apparatus.

[0071] Fig. 7 is the configuration at the time of administering, that is, setting and changing the public key fix-

edly saved in a public key acquisition unit 12C in a finger print acquisition apparatus 12. An administration terminal 11 is a computer system such as a personal computer and a workstation, where an administration S/W 11A operates. The finger print acquisition apparatus 12 is composed of a finger print information acquisition unit 12A and an encryption processing unit 12B, a public key acquisition unit 12C, and an administration unit 12D.

[0072] The administration S/W 11A in the administration terminal 11 issues authentication request of an administrator to the finger print acquisition apparatus 12 so as to execute setting of the public key. Although an administrator authentication unit 12D1 in an administration unit 12D in the finger print acquisition apparatus 12 acquires administrator's finger print from the finger print information acquisition unit 7A and performs finger print matching of the administrator, the administrator authentication unit 12D1 may become in such a condition that the unit 12D1 cannot identify the administrator as the valid administrator. This corresponds to a case that the finger print itself is lost due to an injury of the administrator. In this case, although the administration S/W 11A instructs an initializer authentication unit 12D2 in the administration unit 12D in the finger print acquisition apparatus 12 to perform initialization, the S/W 11A performs the authentication of the initializer with means, being set beforehand, such as a password. The initializer authentication unit 12D2 performs only the authentication of the initializer, only the initialization of the finger print acquisition apparatus is executed by the authentication of the initializer authentication unit 12D2.

[0073] In this manner, by providing the authentication means for an initializer separately from an ordinary administrator, there are such effects that it is possible to perform only the initialization if an administrator cannot be authenticated and suddenly becomes absent, and furthermore to prevent a person not having the initialization authority from invalidly performing the initialization.

Embodiment 5.

[0074] Fig. 8 shows an authentication server where means for finding invalid authentication is applied to the above-described authentication server so as to enhance reliability. An authentication server 13 is a computer system such as a personal computer and a workstation, which is composed of a logging unit 13D, an authentication controller 13A, an encryption processing unit 13C, and an authentication information database 13B.

[0075] The logging unit 13D in the authentication server 13 logs a matching rate that is the result of matching biometrics at the time of the user authentication. In addition, the logging unit 13D confirm that a matching rate at this time does not change more than or equal to a preset value determined by the administrator by comparing the matching rate at this time with the average matching rate at the time of identifying a user as the principal until the previous occasion if the authentication controller

13A does not identifies the user as the principal at the time of the user authentication. If the matching rate changes more than or equal to a fixed value, the logging unit 13D increases the number of failure times. If the number of failure times reaches the value more than or equal to a fixed value determined by the administrator, the logging unit 13D informs the administrator, who is registered beforehand, and the user herself/himself of the failure.

[0076] Since this structure informs the administrator and the user, who is personated, of the abnormal result of the matching that is unique in biometrics authentication, it is possible to early find the invalid authentication and to keep the high security of the system.

[0077] In addition, since biometrics information becomes information different every acquisition even if matching rates are the same, it is stochastically very small that biometrics information acquired in the past coincides with the new biometrics information. An invalidity-finding structure using this characteristic of the biometrics authentication will be described.

[0078] The logging unit 13D in the authentication server 13 that is shown in Fig. 8 compares a matching rate at this time with the matching rate at the time of identifying a user as the principal until the previous occasion and confirms that both matching rates are the same if the authentication controller 13A identifies the user as the principal at the time of the user authentication. If the matching rates are the same and a message digest of the biometrics information is not saved, the logging unit 13D informs the authentication controller 13A of making the user authentication unsuccessful, and the authentication controller 13A makes the result of the authentication unsuccessful. At the same time, the logging unit 13D saves the message digest of the biometrics information with the matching rate. If the matching rates are the same and the message digest of the biometrics information is saved, the logging unit 13D calculates a message digest of the biometrics information at this time, compares this message digest with the message digest of the biometrics information at the same matching rate in the past. If both message digest are different from each other, the logging unit 13D identifies the user as the principal, but, if both coincide with each other, the logging unit 13D informs the authentication controller 13A of making the user authentication unsuccessful since there is a possibility of masquerade. The authentication controller 13A makes the result of the authentication unsuccessful. The logging unit 13D increases the number of failure times at the same matching rate if the authentication is made unsuccessful due to coincidence of the matching rate and message digest, and, if this number of failure times reaches a value more than or equal to the fixed value determined by the administrator, the logging unit 13D informs the administrator and the user herself/himself that are registered beforehand.

[0079] Since this structure informs the administrator and the user, who is personated, of such an abnormal

state that it is considered to be the masquerade caused by leakage of the biometrics information, it is possible to early find the invalid authentication and to keep the high security of the system. In addition, there are such effects that it is possible to reduce a storage area since an object which the logging unit 13D saves is the message digest of the biometrics information at the time of the same matching rate after the second occasion, and that it is possible to shorten the time consumed for comparison in comparison with the comparison, performed by using biometrics information itself, because of the comparison performed by using the message digests.

[0080] As described above, according to the present invention, there is such an effect that it is possible to securely protect the user's personal privacy, which is the finger print information that is the biometrics information, in a style of reflecting user's intention since the finger print information is transferred over the network in such a condition that only the authentication server, which the user assigned, can decode the finger print information, and it is possible to prevent invalid authentication information from being reused since the date and time when the authentication information was created can be confirmed in the authentication server 3, and to keep the security of the system high since the authentication request side can confirm whether the user is authenticated by the authentication server.

[0081] Furthermore, although a user can instruct a public key of the authentication server, there is no problem on security even if the floppy disk, magnetic card, or IC card, which saves this public key, is lost or stolen, and the user can receive the personal authentication with a substitute, which saves the same public key or the same article. There is another effect that it is unnecessary to perform processing such as special notification and re-issue at the time of loss and burglar and it is possible to lighten the administration load.

[0082] In addition, since the present invention creates random numbers, used for creating the common key, from the biometrics information acquired, it is possible to generate the random numbers irrelevant to the number of authentication times and the time, and to construct a system that is strong on security against the decoding of the common key.

[0083] Furthermore, by providing the authentication means for an initializer separately from an ordinary administrator, there are such effects that it is possible to perform the initialization even if an administrator suddenly becomes absent, and furthermore to prevent a person not having the initialization authority from invalidly performing the initialization.

[0084] Moreover, since the authentication server logs at the time of the user authentication and informs a person, who is registered beforehand, of the abnormal result of the matching that is unique in biometrics authentication, it is possible to early find the invalid authentication and to keep the high security of the system.

Claims

1. A remote authentication system in which an authentication server (3), a computer system (4) having applications that require personal authentication, and a user terminal (5) are each connected to a network (2), and which authenticates a user using the user terminal (5);
 wherein at least one or a plurality of types of biometrics acquisition apparatuses (6) are connected to the user terminal (5);
 the biometrics acquisition apparatus (6) encrypts user's biometrics information acquired at the time of authentication, with a common key in a common key encryption method; and transfers encrypted biometrics information as authentication information to the user terminal (5);
 the user terminal (5) transfers the authentication information added with a user ID to the computer system (4); and
 the computer system (4) transfers the authentication information to the authentication server (3);

characterized in that:

the biometrics acquisition apparatus (6) acquires date and time information, creates a message digest by connecting date and time information with the common key, encrypts the created message digest with the common key, encrypts the common key with a public key acquired from the authentication server (3), and transfers the encrypted message digest, date and time information and the encrypted common key as the authentication information to the user terminal (5); the authentication server (3) has a pair of the public encryption method public key and secret key, publishes the public key, and conceals the secret key, decodes the received encrypted common key with the secret key to obtain a decoded common key, decodes the received encrypted message digest with the decoded common key, creates a message digest by connecting received date and time information with the decoded common key, confirms the validity of the date and time of preparing the authentication information by comparing the created message digest with the decoded message digest, decodes the received encrypted biometrics information with the decoded common key, authenticates the user by matching the decoded biometrics information and biometrics information saved in the authentication server (3), encrypts a message digest of a result of authentication with the secret key, and transfers the encrypted message digest of the result of authentication and the result of authentication to the computer system (4).

2. A remote authentication system according to claim 1, wherein the user terminal (5) includes the computer system (4), and transfers the authentication information to the authentication server (3); and the authentication server (3) transfers the encrypted message digest resulting from authentication and the result of authentication to the user terminal (5).

3. A remote authentication system in which an authentication server (3), a computer system (4) having applications that require personal authentication, and a user terminal (5) are each connected to a network (2), and which authenticates a user using the user terminal (5);

wherein at least one or a plurality of types of biometrics acquisition apparatuses (6) are connected to the user terminal (5);

the biometrics acquisition apparatus (6) transfers user's biometrics information acquired at the time of authentication to the user terminal (5),

the user terminal (5) encrypts received user's biometrics information with a common key in a common key encryption method; and transfers the encrypted user's biometrics information added with a user ID as authentication information to the computer system (4); and

the computer system (4) transfers the authentication information to the authentication server (3);

characterized in that:

the user terminal (5) acquires date and time information, creates a message digest by connecting date and time information with the common key, encrypts the created message digest with the common key, encrypts the common key with a public key acquired from the authentication server (3), and transfers the encrypted message digest, date and time information and the encrypted common key as the authentication information to the computer system (4);

the authentication server (3) has a pair of the public encryption method public key and secret key, publishes the public key, and conceals the secret key, decodes the received encrypted common key with the secret key to obtain the decoded common key, decodes the received encrypted message digest with the decoded common key, creates a message digest by connecting received date and time information with the decoded common key, confirms the validity of the date and time of preparing the authentication by comparing the created message digest with the decoded message digest, decodes the received encrypted biometrics information with the decoded common key, authenticates the user by matching the decoded biometrics information and biometrics information saved in

the authentication server (3), encrypts a message digest of a result of authentication with the secret key, and transfers the encrypted message digest of the result of authentication and the result of authentication to the computer system (4).

4. The remote authentication system according to any one of claims 1 to 3, **characterized in that** user terminal (5) uses biometrics information as a part or all of random numbers for creating the common key when, at the time of authentication, the user terminal creates the common key in a common key encryption method for encrypting the user's biometrics information acquired.

5. The remote authentication system according to any one of claims 1 to 3, **characterized in that** the biometrics acquisition apparatus (12) includes an authentication unit (12D1) of an administrator administering the biometrics acquisition apparatus (12) and an authentication unit (12D2) of an initializer initializing the biometrics acquisition apparatus; and wherein the two authentication units (12D1, D2) perform authentication separately, and the biometrics acquisition apparatus (12) performs initialization with authentication of the initializer even if the administrator is not authenticated.

6. A remote authentication system according to any one of claims 1 to 3, wherein the authentication server (3) newly saves an average matching rate calculated from a matching rate which is a result of matching transferred biometrics information with biometrics information saved in the authentication server (3) when the user is verified as the principal, and an average matching rate saved in the authentication server (3); compares a matching rate which is a result of matching transferred biometrics information with biometrics information saved in the authentication server (3), with the average matching rate saved in the authentication server (3), when the user isn't verified as the principal, increments the number of failures if a variation between the matching rate and the average matching rate is larger than a predetermined threshold value, and reports to the registered person if the number of failures is larger than the established threshold value.

7. A remote authentication system according to any one of claims 1 to 3, wherein the authentication server (3) calculates a matching rate by matching biometrics information in authentication information at this time and biometrics information saved in the authentication server (3) and saves the matching rate into the

authentication server (3);
 does not authenticate a user as the principal if the matching rate at this time is equal to a plurality of matching rates saved in the authentication server (3) when authentication was successful at the previous time, and if a message digest of biometrics information is not saved in the authentication server (3), and saves a message digest of biometrics information of authentication information at this time with the matching rate at this time;
 authenticates a user as the principal if the matching rate at this time is equal to a plurality of matching rates saved in the authentication server (3) when authentication was successful at the previous time, and if a message digest of biometrics information is not equal to a plurality of message digests saved when authentication was successful at the previous time, and saves a message digest of biometrics information of authentication information at this time with the matching rate at this time;
 does not authenticate a user as the principal if the matching rate at this time is equal to a plurality of matching rates saved in the authentication server (3) when authentication was successful at the previous time, and if the message digest of biometrics information at this time is equal to one of the message digests when authentication was successful at the previous time, and increments the number of failures, and reports to the registered person if the number of failures is larger than the established threshold value.

Patentansprüche

1. System zur entfernten Authentifikation, bei dem ein Authentifikationsserver (3), ein Computer-system (4) mit Anwendungen, die eine persönliche Authentifikation erfordern, und ein Benutzerendgerät (5) jeweils mit einem Netzwerk (2) verbunden sind, und das einen das Benutzerendgerät (5) verwendenden Benutzer authentifiziert;
 wobei zumindest eine oder mehrere Typen von Vorrichtungen (6) zur Gewinnung biometrischer Merkmale mit dem Benutzerendgerät (5) verbunden sind; die Vorrichtung (6) zur Gewinnung biometrischer Merkmale Informationen über biometrische Merkmale des Benutzers, die zu der Zeit der Authentifikation gewonnen wurden, mit einem gemeinsamen Schlüssel in einem Verschlüsselungsverfahren mit gemeinsamem Schlüssel verschlüsselt; und verschlüsselte biometrische Informationen als Authentifikationsinformationen zu dem Benutzerendgerät (5) überträgt;
 das Benutzerendgerät (5) die Authentifikationsinformationen mit einem hinzugefügten Benutzer-ID zu dem Computersystem (4) überträgt; und das Computersystem (4) die Authentifikationsinfor-

mationen zu dem Authentifikationsserver (3) überträgt;

dadurch gekennzeichnet, dass:

5 die Vorrichtung (6) zur Gewinnung biometrischer Merkmale Datums- und Zeitinformationen erwirbt, eine Nachrichtenauswahl durch Verbinden von Datums- und Zeitinformationen mit dem gemeinsamen Schlüssel schafft, die geschaffene Nachrichtenauswahl mit dem gemeinsamen Schlüssel verschlüsselt, den gemeinsamen Schlüssel mit einem öffentlichen Schlüssel verschlüsselt, der von dem Authentifikationsserver (3) erhalten wurde, und die verschlüsselte Nachrichtenauswahl, Datums- und Zeitinformationen und den verschlüsselten gemeinsamen Schlüssel als die Authentifikationsinformationen zu dem Benutzerendgerät (5) überträgt;
 10 der Authentifikationsserver (3) ein Paar aus dem öffentlichen Schlüssel des öffentlichen Verschlüsselungsverfahrens und Geheimschlüssel hat, den öffentlichen Schlüssel veröffentlicht und den Geheimschlüssel verbirgt, den empfangenen verschlüsselten gemeinsamen Schlüssel mit dem Geheimschlüssel decodiert, um einen decodierten gemeinsamen Schlüssel zu erhalten, die empfangene verschlüsselte Nachrichtenauswahl mit dem decodierten gemeinsamen Schlüssel decodiert, eine Nachrichtenauswahl schafft durch Verbinden empfangener Datums- und Zeitinformationen mit dem decodierten gemeinsamen Schlüssel, die Gültigkeit des Datums und der Zeit der Bildung der Authentifikationsinformationen bestätigt durch Vergleichen der geschaffenen Nachrichtenauswahl mit der decodierten Nachrichtenauswahl, die empfangenen verschlüsselten biometrischen Informationen mit dem decodierten gemeinsamen Schlüssel decodiert, den Benutzer authentifiziert durch Anpassen der decodierten biometrischen Informationen und der in dem Authentifikationsserver (3) übertragenen biometrischen Informationen, eine Nachrichtenauswahl eines Ergebnisses der Authentifikation mit dem Geheimschlüssel verschlüsselt und die verschlüsselte Nachrichtenauswahl des Ergebnisses der Authentifikation und das Ergebnis der Authentifikation zu dem Computersystem (4) überträgt.

2. System zur entfernten Authentifikation nach Anspruch 1,
 bei dem das Benutzerendgerät (5) das Computer-system (4) enthält und die Authentifikationsinformationen zu dem Authentifikationsserver (3) überträgt; und
 50 der Authentifikationsserver (3) die verschlüsselte Nachrichtenauswahl, die sich aus der Authentifikation ergibt, und das Ergebnis der Authentifikation zu

dem Benutzerendgerät (5) überträgt.

3. System zur entfernten Authentifikation, bei dem ein Authentifikationsserver (3), ein Computersystem (4) mit Anwendungen, die eine persönliche Authentifikation erfordern, und ein Benutzerendgerät (5) jeweils mit einem Netzwerk (2) verbunden sind, und das einen das Benutzerendgerät (5) verwendenden Benutzer authentifiziert; wobei zumindest ein oder mehrere Typen von Vorrichtungen (6) zur Gewinnung biometrischer Merkmale mit dem Benutzerendgerät (5) verbunden sind; die Vorrichtung (6) zur Gewinnung biometrischer Merkmale Informationen über biometrische Merkmale des Benutzers, die zu der Zeit der Authentifikation gewonnen wurden, zu dem Benutzerendgerät (5) überträgt, das Benutzerendgerät (5) empfangene Informationen über biometrische Merkmale des Benutzers mit einem gemeinsamen Schlüssel durch ein Verschlüsselungsverfahren mit gemeinsamem Schlüssel verschlüsselt und die verschlüsselten Informationen über biometrische Merkmale des Benutzers, zu denen ein Benutzer-ID hinzugefügt ist, als Authentifikationsinformationen zu dem Computersystem (4) überträgt; und das Computersystem (4) die Authentifikationsinformationen zu dem Authentifikationsserver (3) überträgt;

dadurch gekennzeichnet, dass:

das Benutzerendgerät (5) erwirbt Datums- und Zeitinformationen, schafft eine Nachrichtenauswahl durch Verbinden von Datums- und Zeitinformationen mit dem gemeinsamen Schlüssel, verschlüsselt die geschaffene Nachrichtenauswahl mit dem gemeinsamen Schlüssel, verschlüsselt den gemeinsamen Schlüssel mit einem öffentlichen Schlüssel, der von dem Authentifikationsserver (3) erhalten wurde, und überträgt die verschlüsselte Nachrichtenauswahl, Datums- und Zeitinformationen und den verschlüsselten gemeinsamen Schlüssel als die Authentifikationsinformationen zu dem Computersystem (4);

der Authentifikationsserver (3) ein Paar des öffentlichen Schlüssels eines öffentlichen Verschlüsselungsverfahrens und Geheimschlüssel hat, den öffentlichen Schlüssel veröffentlicht und den Geheimschlüssel geheim hält, den empfangenen verschlüsselten gemeinsamen Schlüssel mit dem Geheimschlüssel decodiert, um den decodierten gemeinsamen Schlüssel zu erhalten, die empfangene verschlüsselte Nachrichtenauswahl mit dem decodierten gemeinsamen Schlüssel decodiert, eine Nachrichtenauswahl schafft durch Verbinden empfangener Datums- und Zeitinformationen mit dem decodier-

ten gemeinsamen Schlüssel, die Gültigkeit des Datums und der Zeit der Bildung der Authentifikation bestätigt durch Vergleichen der geschaffenen Nachrichtenauswahl mit der decodierten Nachrichtenauswahl, die empfangenen verschlüsselten biometrischen Informationen mit dem decodierten gemeinsamen Schlüssel decodiert, den Benutzer authentifiziert durch Anpassen der decodierten biometrischen Informationen und der in den Authentifikationsserver (3) übertragenen biometrischen Informationen, eine Nachrichtenauswahl eines Ergebnisses der Authentifikation mit dem Geheimschlüssel verschlüsselt und die verschlüsselte Nachrichtenauswahl des Ergebnisses der Authentifikation und das Ergebnis der Authentifikation zu dem Computersystem (4) überträgt.

4. System zur entfernten Authentifikation nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet, dass** das Benutzerendgerät (5) biometrische Informationen als einen Teil von oder alle Zufallszahlen zum Schaffen des gemeinsamen Schlüssels verwendet, wenn zu der Zeit der Authentifikation das Benutzerendgerät den gemeinsamen Schlüssel in einem Verschlüsselungsverfahren mit gemeinsamem Schlüssel zum Verschlüsseln der gewonnenen biometrischen Informationen des Benutzers schafft.

5. System zur entfernten Authentifikation nach einem der Ansprüche 1 bis 3, **dadurch gekennzeichnet, dass** die Vorrichtung (12) zur Gewinnung biometrischer Merkmale eine Authentifikationseinheit (12D1) einer Verwaltungsvorrichtung, die die Vorrichtung (12) zur Gewinnung biometrischer Merkmale und eine Authentifikationseinheit (12D2) einer Initialisierungsvorrichtung, die die Vorrichtung zur Gewinnung biometrischer Merkmale initialisiert, verwaltet, enthält; und wobei die zwei Authentifikationseinheiten (12D1, D2) eine Authentifikation getrennt durchführen und die Vorrichtung (12) zur Gewinnung biometrischer Merkmale eine Initialisierung mit der Authentifikation der Initialisierungsvorrichtung durchführt, selbst wenn die Verwaltungsvorrichtung nicht authentifiziert ist.

6. System zur entfernten Authentifikation gemäß einem der Ansprüche 1 bis 3, bei dem der Authentifikationsserver (3) eine Durchschnittsanpassungsrate neu speichert, die anhand einer Anpassungsrate berechnet wurde, die ein Ergebnis der Anpassung übertragener biometrischer Informationen an biometrische Informationen, die in dem Authentifikationsserver (3) gespeichert sind, ist, wenn der Benutzer als der Prinzipal verifiziert ist, und eine Durchschnittsanpassungsrate, die in dem Authentifikationsserver (3) gespeichert ist; eine Anpassungsrate, die ein Ergebnis der Anpas-

sung übertragener biometrischer Informationen mit in den Authentifikationsserver (3) gespeicherten biometrischen Informationen ist, mit der in den Authentifikationsserver (3) gespeicherten Durchschnittsanpassungsrate vergleicht, wenn der Benutzer nicht als der Prinzipal verifiziert wird, die Anzahl von Fehlschlägen erhöht, wenn eine Veränderung zwischen der Anpassungsrate und der Durchschnittsanpassungsrate größer als ein vorbestimmter Schwellenwert ist, und zu der registrierten Person berichtet, wenn die Anzahl von Fehlschlägen größer als der errichtete Schwellenwert ist.

7. System für entfernte Authentifikation gemäß einem der Ansprüche 1 bis 3, bei dem der Authentifikationsserver (3)
- eine Anpassungsrate durch Anpassung biometrischer Informationen in Authentifikationsinformationen zu dieser Zeit und in den Authentifikationsserver (3) gespeicherter biometrischer Informationen berechnet und die Anpassungsrate in dem Authentifikationsserver (3) speichert;
- einen Benutzer nicht als den Prinzipal authentifiziert, wenn die Anpassungsrate zu dieser Zeit gleich mehreren Anpassungsraten ist, die in dem Authentifikationsserver (3) gespeichert sind, wenn die Authentifikation zu der vorhergehenden Zeit erfolgreich war, und wenn eine Nachrichtenauswahl von biometrischen Informationen nicht in dem Authentifikationsserver (3) gespeichert ist, und eine Nachrichtenauswahl von biometrischen Informationen von Authentifikationsinformationen zu dieser Zeit mit der Anpassungsrate zu dieser Zeit speichert;
- einen Benutzer als den Prinzipal authentifiziert, wenn die Anpassungsrate zu dieser Zeit gleich mehreren Anpassungsraten ist, die in dem Authentifikationsserver (3) gespeichert sind, wenn die Authentifikation zu der vorhergehenden Zeit erfolgreich war, und wenn eine Nachrichtenauswahl von biometrischen Informationen nicht gleich mehreren Nachrichtenauswahlen ist, die gespeichert wurden, wenn die Authentifikation zu der vorhergehenden Zeit erfolgreich war, und eine Nachrichtenauswahl von biometrischen Informationen von Authentifikationsinformationen zu dieser Zeit, mit der Anpassungsrate zu dieser Zeit speichert;
- einen Benutzer nicht als den Prinzipal authentifiziert, wenn die Anpassungsrate zu dieser Zeit gleich mehreren Anpassungsraten ist, die in dem Authentifikationsserver (3) gespeichert sind, wenn die Authentifikation zu der vorhergehenden Zeit erfolgreich war, und wenn die Nachrichtenauswahl von biometrischen Informationen zu dieser Zeit gleich einer der Nachrichtenauswahlen ist, wenn die Authentifikation zu der vorhergehenden Zeit erfolgreich war, und die Anzahl von Fehlschlägen erhöht, und der registrierten Person berichtet, wenn die Anzahl von Fehlschlägen größer ist als der errichtete Schwellenwert.

Revendications

1. Système d'authentification à distance, dans lequel un serveur d'authentification (3), un système d'ordinateur (4), ayant des applications demandant une authentification personnelle, et un terminal utilisateur (5) sont chacun connectés à un réseau (2), et qui authentifie un utilisateur utilisant le terminal utilisateur (5) ;
dans lequel au moins l'un d'une pluralité de types de dispositifs d'acquisition biométriques (6) sont connectés au terminal utilisateur (5) ;
le dispositif d'acquisition biométrique (6) chiffre une information biométrique sur l'utilisateur, acquise au moment de l'authentification, avec une clé commune dans un procédé de chiffrement par clé commune ; et transfère l'information biométrique chiffrée, en tant qu'information authentification, au terminal utilisateur (5) ;
le terminal utilisateur (5) transfère l'information d'authentification ajoutée avec un ID utilisateur au système d'ordinateur (4) ; et
le système d'ordinateur (4) transfère l'information d'authentification au serveur d'authentification (3) ;
caractérisé en ce que
le dispositif d'acquisition biométrique (6) acquiert une information de date et d'heure, crée un résumé de message en connectant l'information de date et d'heure à la clé commune, chiffre le résumé de message créé avec la clé commune, chiffre la clé commune avec une clé publique acquise auprès du serveur d'authentification (3), et transfère le résumé de message chiffré, l'information de date et d'heure et la clé commune chiffrée, en tant qu'information d'authentification, au terminal utilisateur (5) ;
le serveur d'authentification (3) comprend une paire de clé publique et de clé secrète pour un procédé de chiffrement public, publie la clé publique, et dissimule la clé secrète, décode la clé commune chiffrée reçue avec la clé secrète pour obtenir une clé commune décodée, décode le résumé de message chiffré reçu avec la clé commune décodée, crée un résumé de message en connectant l'information de date et d'heure reçue avec la clé commune décodée, confirme la validité de la date et de l'heure de préparation de l'information d'authentification en comparant le résumé de message créé au résumé de message décodé, décode l'information biométrique chiffrée ayant été reçue avec la clé commune décodée, authentifie l'utilisateur par coïncidence entre l'information biométrique décodée et l'information biométrique sauvegardée dans le serveur d'authentification (3), chiffre un résumé de message d'un résultat d'authentification avec la clé secrète, et transfère le résumé de message chiffré du résultat d'authentification et le résultat d'authentification, au système d'ordinateur (4).

2. Système d'authentification à distance selon la revendication 1, dans lequel le terminal utilisateur (5) comprend le système d'ordinateur (4), et transfère l'information d'authentification au serveur d'authentification (3) ; et le serveur d'authentification (3) transfère le résumé de message chiffré, résultant de l'authentification et le résultat d'authentification, au terminal utilisateur (5).
3. Système d'authentification à distance, dans lequel un serveur d'authentification (3), un système d'ordinateur (4) ayant des applications qui demandent une authentification personnelle, et un terminal utilisateur (5) sont chacun connectés à un réseau (2), et qui authentifie un utilisateur utilisant le terminal utilisateur (5) ; dans lequel au moins l'un ou une pluralité de types de dispositifs d'acquisition biométriques (6) sont connectés au terminal utilisateur (5) ; le dispositif d'acquisition biométrique (6) transfère une information biométrique sur l'utilisateur, ayant été acquise au moment de l'authentification, au terminal utilisateur (5), le terminal utilisateur (5) chiffre l'information biométrique de l'utilisateur ayant été reçue, avec une clé commune dans un procédé de chiffrement à clé commune ; et transfère l'information biométrique de l'utilisateur, ayant été chiffrée, ajoutée à un ID utilisateur, en tant qu'information d'authentification, au système d'ordinateur (4) ; et le système d'ordinateur (4) transfère l'information d'authentification au serveur d'authentification (3) ; **caractérisé en ce que** le terminal utilisateur (5) acquiert une information de date et d'heure, crée un résumé de message en connectant l'information de date et d'heure à la clé commune, chiffre le résumé de message créé avec la clé commune, chiffre la clé commune avec une clé publique acquise auprès du serveur d'authentification (3), et transfère le résumé de message chiffré, l'information de date et d'heure et la clé commune chiffrée en tant qu'information d'authentification, au système d'ordinateur (4) ; le serveur d'authentification (3) comprend une paire de clé publique et de clé secrète du procédé de chiffrement public, publie la clé publique, et dissimule la clé secrète, décode la clé commune chiffrée reçue avec la clé secrète pour obtenir la clé commune décodée, décode le résumé de message chiffré reçu avec la clé commune décodée, crée un résumé de message en connectant l'information de date et d'heure reçue avec la clé commune décodée, confirme la validité de la date et de l'heure de la préparation de l'authentification par comparaison entre le résumé de message créé et le résumé de message décodé, décode l'information biométrique chiffrée
- reçue, avec la clé commune décodée, authentifie l'utilisateur par mise en coïncidence entre l'information biométrique décodée et l'information biométrique sauvegardée dans le serveur d'authentification (3), chiffre un résumé de message d'un résultat d'authentification avec la clé secrète, et transfère le résumé de message chiffré du résultat d'authentification et le résultat d'authentification, au système d'ordinateur (4).
4. Système d'authentification à distance selon l'une quelconque des revendications 1 à 3, **caractérisé en ce que** le terminal utilisateur (5) fait utilisation d'une information biométrique en tant que partie ou totalité des nombres aléatoires pour créer la clé commune lorsque, au moment de l'authentification, le terminal utilisateur crée la clé commune dans un procédé de chiffrement à clé commune, pour chiffrer l'information biométrique de l'utilisateur ayant été acquise.
5. Système d'authentification à distance selon l'une quelconque des revendications 1 à 3, **caractérisé en ce que** le dispositif d'acquisition biométrique (12) inclut une unité d'authentification (12D1) d'un administrateur administrant le dispositif d'acquisition biométrique (12) et une unité d'authentification (12D2) d'un initialiseur initialisant le dispositif d'acquisition biométrique ; et dans lequel les deux unités d'authentification (12D1, D2) accomplissent une authentification séparément et le dispositif d'acquisition biométrique (12) accomplit une initialisation avec l'authentification de l'initialiseur, même si l'administrateur n'est pas authentifié.
6. Système d'authentification à distance selon l'une quelconque des revendications 1 à 3, dans lequel le serveur d'authentification (3) sauvegarde de nouveau un taux de coïncidence moyen, calculé à partir d'un taux de coïncidence qui est un résultat de coïncidence d'une information biométrique transférée avec une information biométrique sauvegardée dans le serveur d'authentification (3), lorsque l'utilisateur est vérifié comme étant le principal, et un taux de coïncidence moyen, sauvegardé dans le serveur d'authentification (3) ; compare un taux de coïncidence qui est un résultat de coïncidence d'une information biométrique transférée avec une information biométrique sauvegardée dans le serveur d'authentification (3), avec le taux de coïncidence moyen sauvegardé dans le serveur d'authentification (3), lorsque l'utilisateur n'est pas vérifié comme étant le principal, incrémente le nombre d'erreurs, si une variation, entre le taux de coïncidence et le taux de coïncidence moyen, est supérieure à une valeur de seuil prédéterminée et rapporte à la personne enregistrée, si le

nombre d'erreurs est supérieur à la valeur de seuil établie.

7. Système d'authentification à distance selon l'une quelconque des revendications 1 à 3, dans lequel le serveur d'authentification (3) :

calculé un taux de coïncidence par coïncidence d'une information biométrique dans une information d'authentification à ce moment et une information biométrique sauvegardée dans le serveur d'authentification (3), et sauvegarde le taux de coïncidence dans le serveur d'authentification (3) ;

n'authentifie pas un utilisateur comme étant le principal si le taux de coïncidence à ce moment est égal à une pluralité de taux de coïncidence sauvegardés dans le serveur d'authentification (3) lorsque l'authentification a été couronnée de succès au moment antérieur et si un résumé de message de l'information biométrique n'est pas sauvegardé dans le serveur d'authentification (3), et sauvegarde un résumé de message d'information biométrique d'information d'authentification à ce moment, avec le taux de coïncidence à ce moment ;

authentifie un utilisateur comme étant le principal, si le taux de coïncidence à ce moment est égal à une pluralité de taux de coïncidence sauvegardés dans le serveur d'authentification (3), lorsque l'authentification avait été couronnée de succès au moment antérieur, et si un résumé de message de l'information biométrique n'est pas égal à une pluralité de résumés de message sauvegardés lorsque l'authentification a été couronnée de succès au moment antérieur, et sauvegarde un résumé de message d'information biométrique d'information d'authentification à ce moment avec le taux d'authentification à ce moment ;

n'authentifie pas un utilisateur comme étant le principal si le taux de coïncidence à ce moment n'est pas égal à une pluralité de taux de coïncidence sauvegardés dans le serveur d'authentification (3), lorsque l'authentification avait été couronnée de succès au moment antérieur, et si le résumé de message de l'information biométrique à ce moment est égal à un des résumés de message lorsque l'authentification avait été couronnée de succès au moment antérieur, et incrémente le nombre d'erreurs, et rapporte à la personne enregistrée si le nombre d'erreurs est supérieur à la valeur de seuil établie.

55

FIG. 1

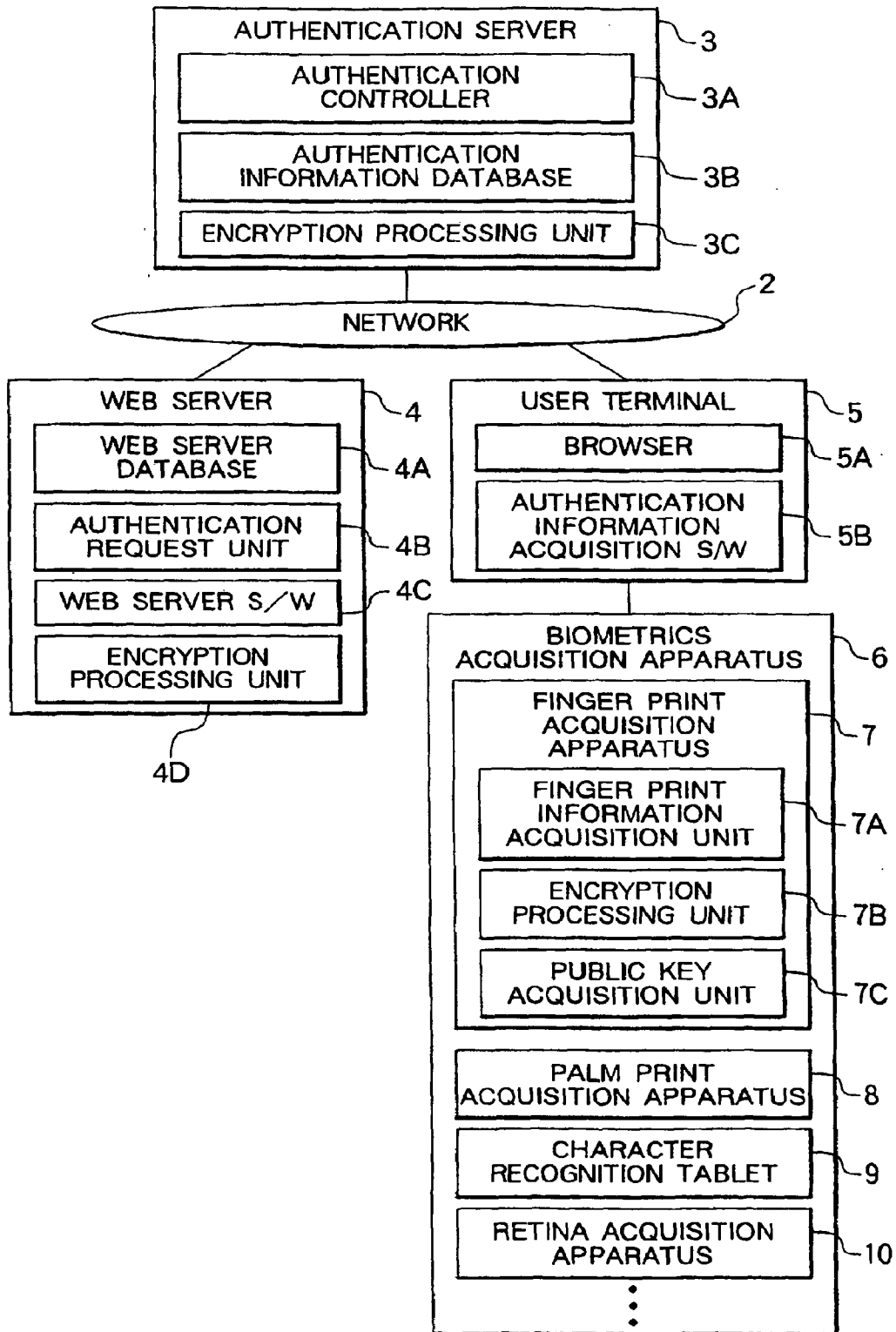


FIG. 2

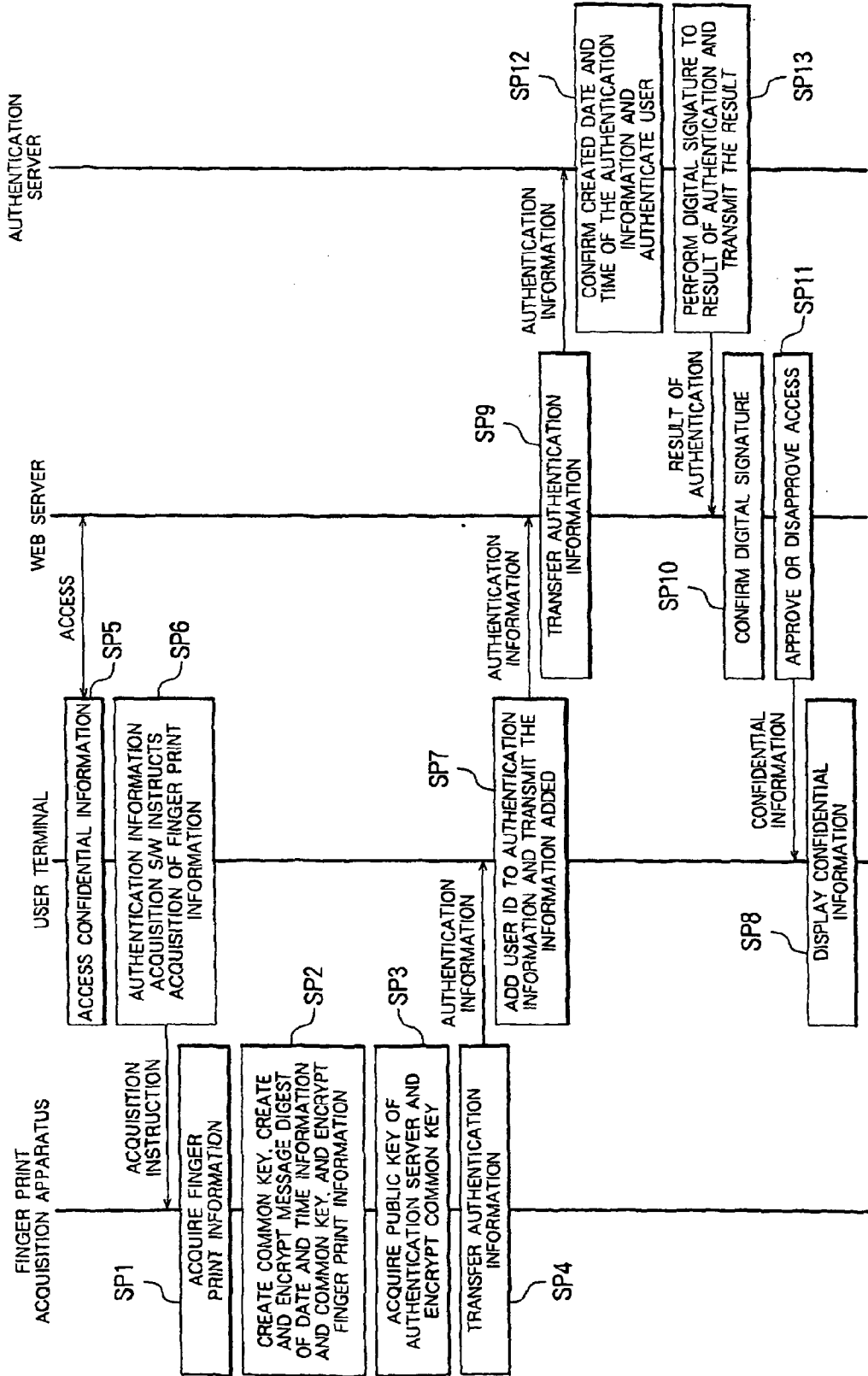


FIG. 3

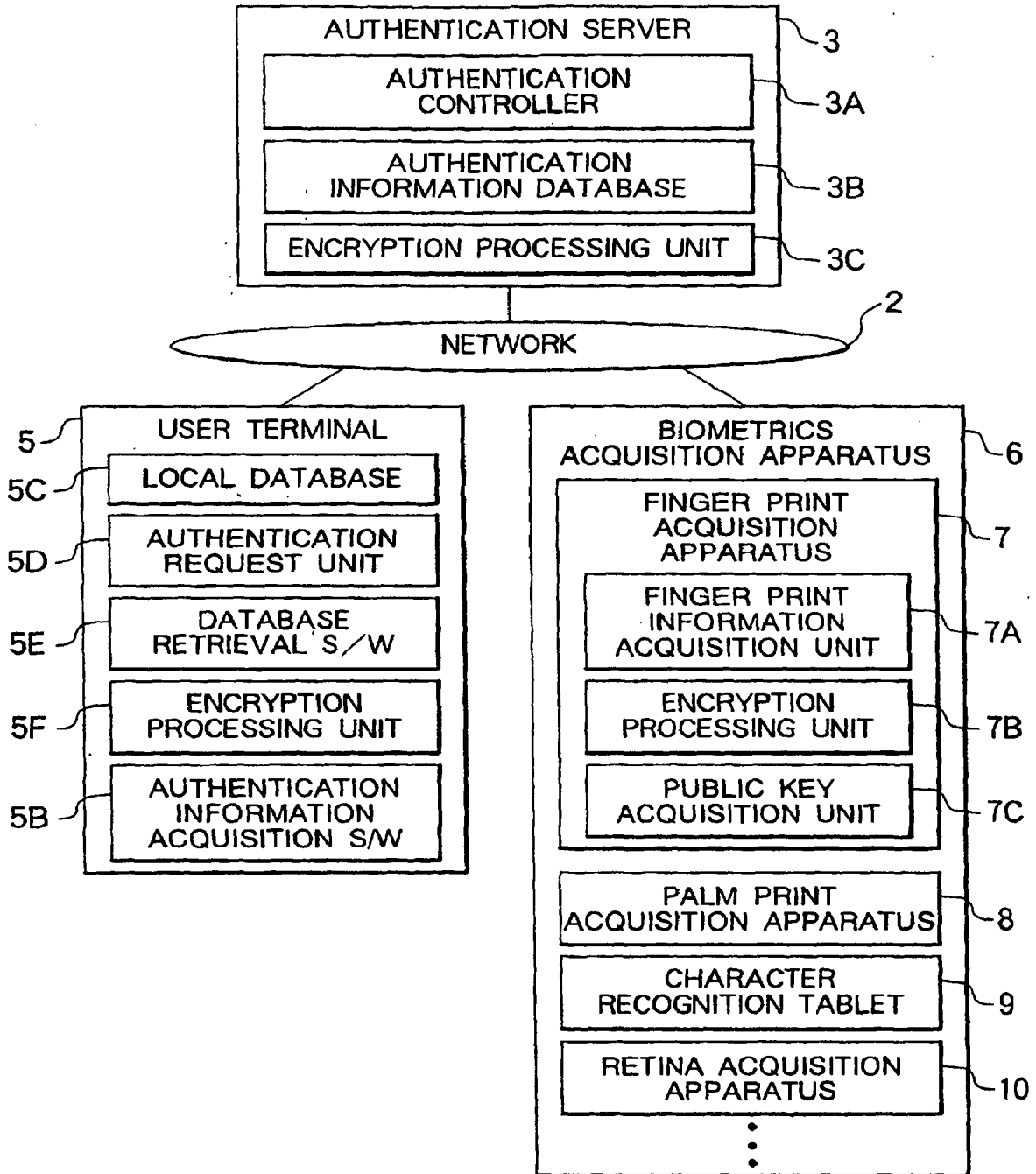


FIG. 4

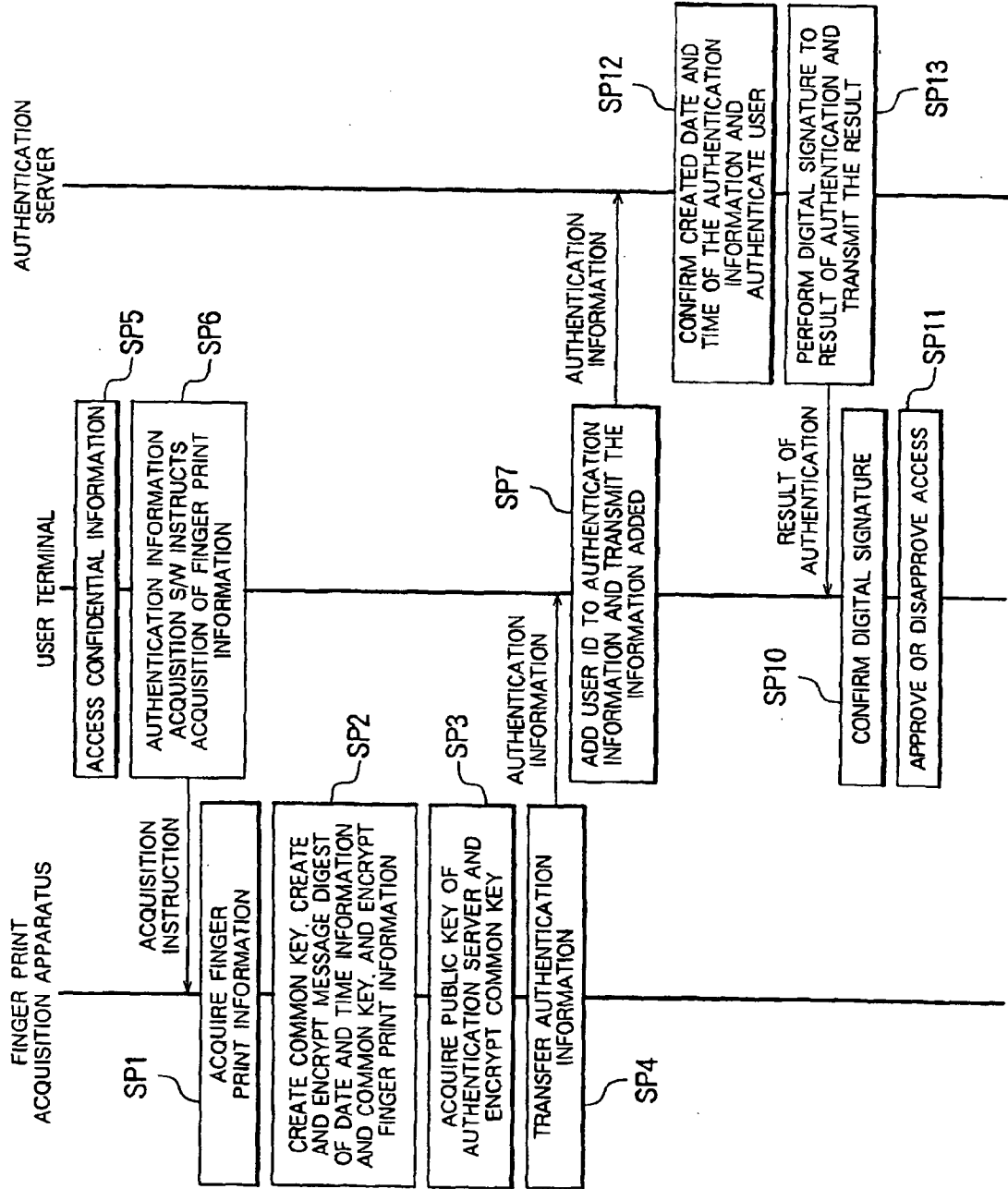


FIG. 5

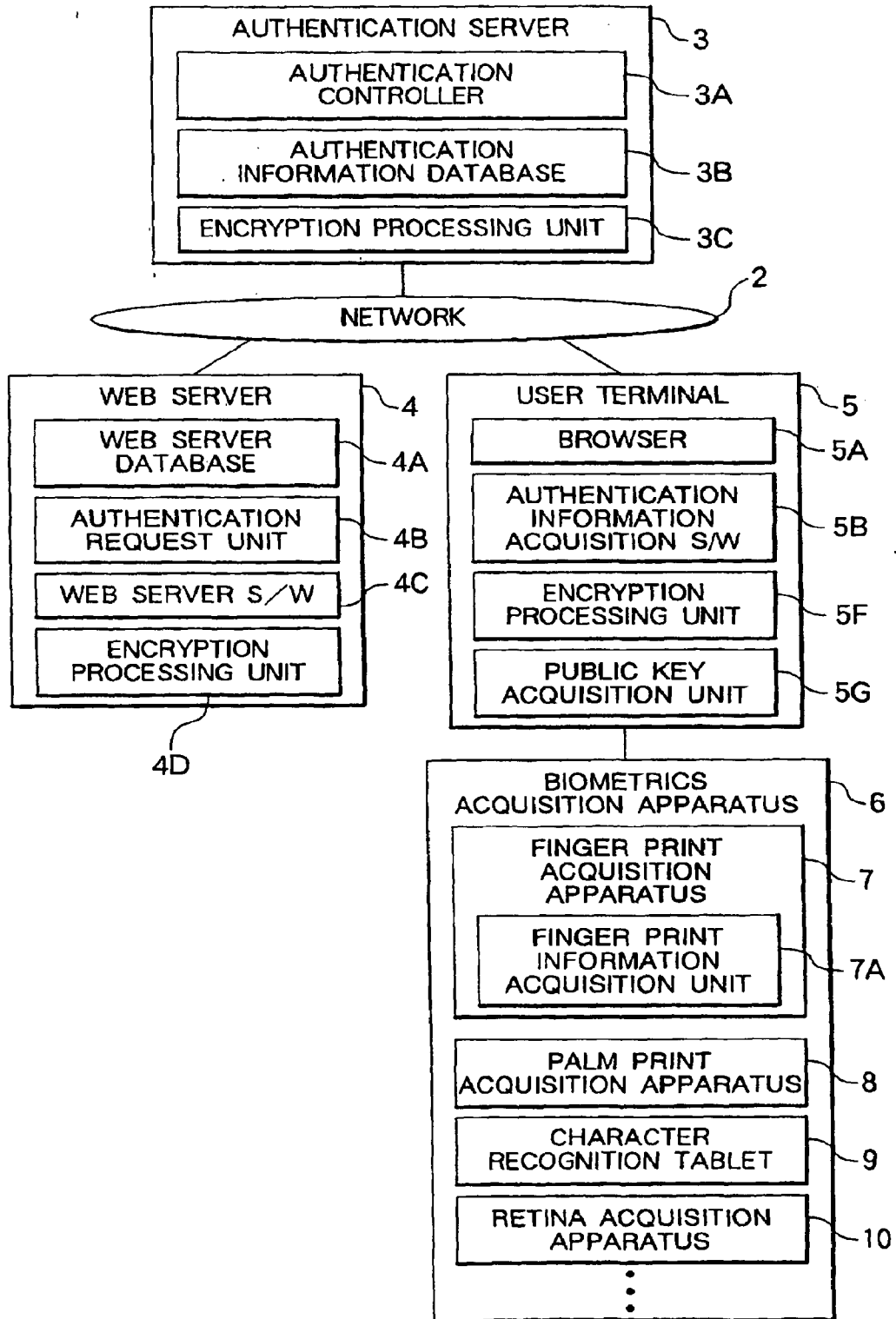


FIG. 6

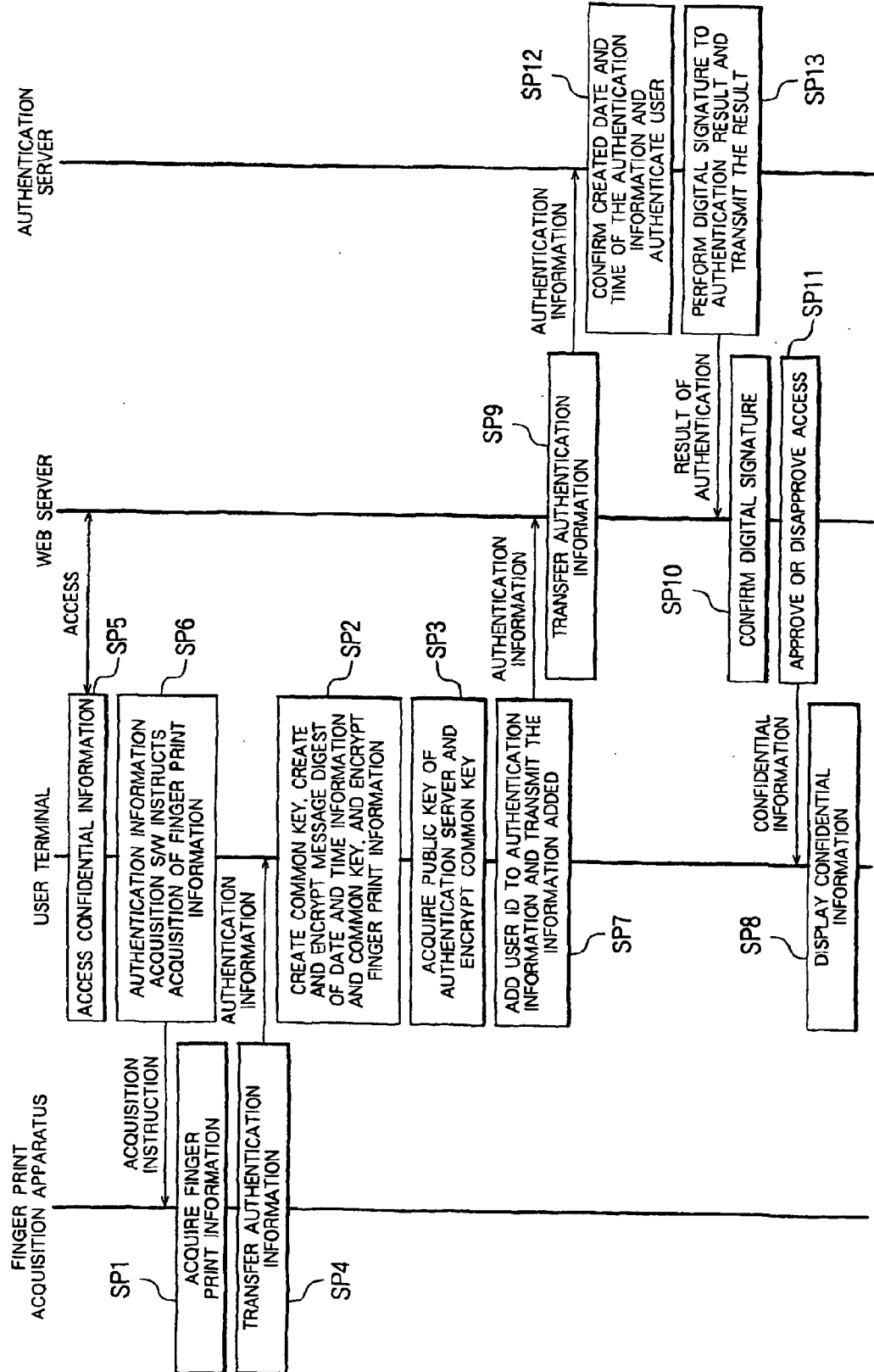


FIG. 7

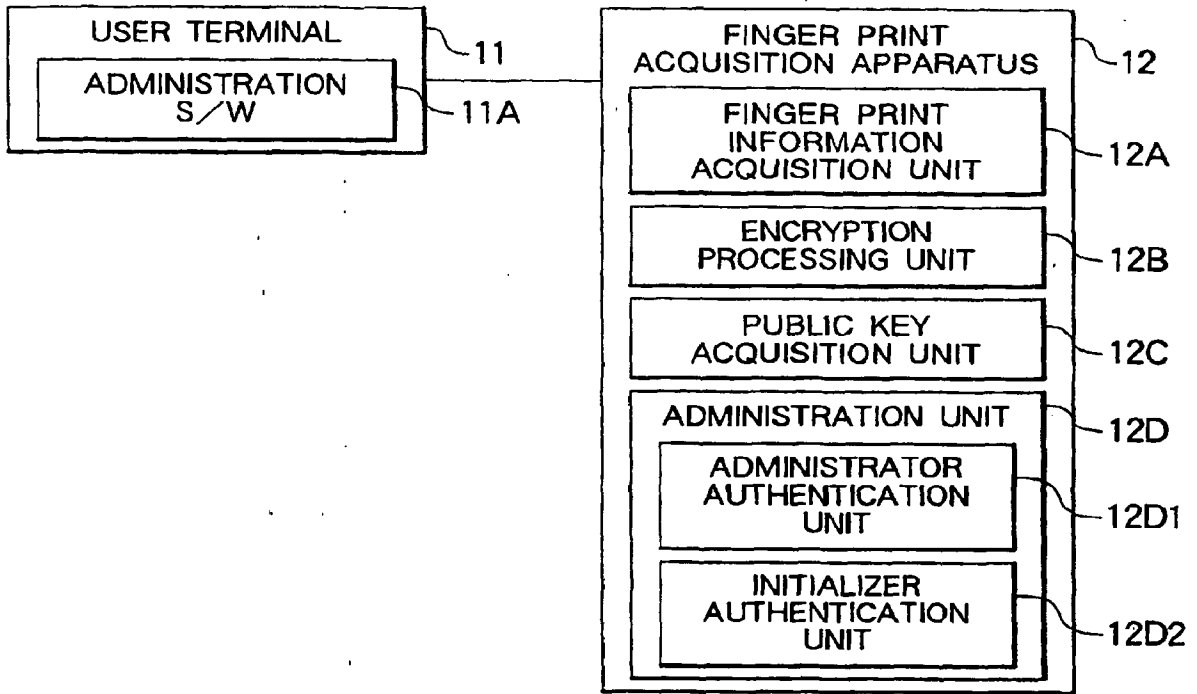
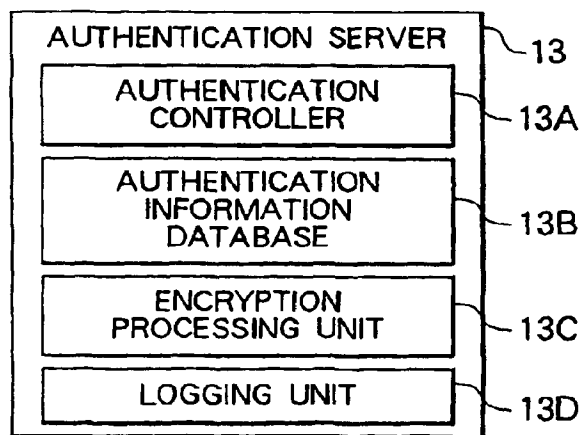


FIG. 8



CORRECTED VERSION

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
21 February 2002 (21.02.2002)

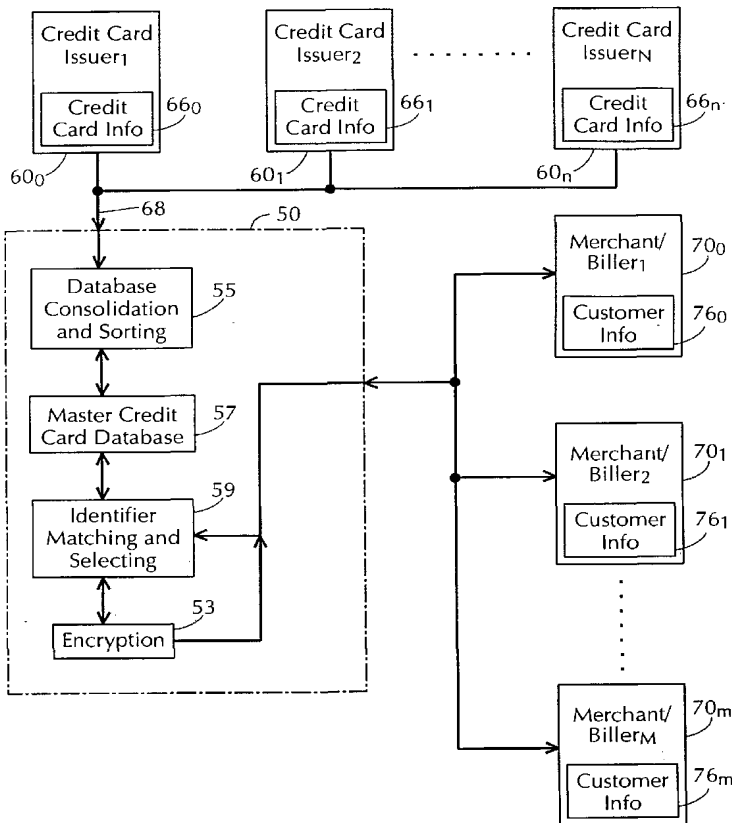
PCT

(10) International Publication Number
WO 02/014985 A3

- (51) International Patent Classification⁷: **G06F 17/60**
- (74) Agents: **YANNEY, Pierre, R.** et al.; Darby & Darby P.C., 805 Third Avenue, New York, NY 10022 (US).
- (21) International Application Number: PCT/US01/25888
- (81) Designated States (*national*): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.
- (22) International Filing Date: 17 August 2001 (17.08.2001)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data: 09/641,073 17 August 2000 (17.08.2000) US
- (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CI, CG, CH, CM, GN, GU, KE, ML, MR, NE, NG, SN, TD, TG).
- (71) Applicant and (72) Inventor: **KERN, Daniel, A.** [US/US]; 201 East 69th Street, New York, NY 10021 (US).

[Continued on next page]

(54) Title: AUTOMATED PAYMENT SYSTEM



(57) Abstract: An automated payment system (50), such as for credit cards, is provided which compiles customer financial account information (76) from a plurality of financial institutions. The system receives account information (66) from the financial institutions, and compiles the information (76) in a central location (55). The system presents financial account information (76) to the customer. The system then receives and stores a selection of at least one of the financial account of the customer and provides the selected financial account information (76) to a merchant, biller or payment processor (70).



WO 02/014985 A3



CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(48) Date of publication of this corrected version:

21 August 2003

Published:

— *with international search report*

(15) Information about Correction:

see PCT Gazette No. 34/2003 of 21 August 2003, Section II

(88) Date of publication of the international search report:

13 June 2002

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

5

10

AUTOMATED PAYMENT SYSTEM

15

FIELD OF THE INVENTION

The present invention relates to computerized billing and payment systems. In particular, the invention relates to an automated credit card payment system that matches a customer's information, fingerprint, retina scan voice, or other biometric measurement and/or a unique personal identifier ("UPI") with financial account information consolidated from multiple financial institutions and selects, or allows customers to select, a financial account for use in paying bills, invoices and other obligations.

25

BACKGROUND OF THE INVENTION

Most companies that provide continual services can automatically bill their customers on a regular basis. To increase customer retention, as well as reliability in payments, and also to avoid the need for repeated billings of past due accounts, companies

increasingly offer customers the option of making payments through the customer's credit card. However, the need for customers to retrieve the credit card they wish to use, coupled with the customer's perception that writing their credit card account number on a bill and mailing it is not secure, hinders many customers from taking advantage of this convenient payment method.

5 Second, when a customer desires to purchase goods or services on the Internet, they usually give the merchant their credit card information as a form of payment. Since there are millions of merchants on the Internet, it is becoming increasingly difficult for the consumer and for credit card organizations to control fraud. From the moment the consumer presses "send" on the merchant's website, their credit card is exposed. Their card number can be
10 intercepted by perpetrators en route to the merchant, or it can be "hacked" from the merchant's database once it is received. In addition, the fact that there are millions of merchants and that that number is growing exponentially, makes it virtually impossible to ensure that the merchant is a legitimate company and not merely in existence to perpetrate credit card fraud.

 Third, when a customer purchases goods or services with a traditional bricks-
15 and-mortar merchant, they must have their credit card with them, and they must give it to the merchant so that the credit card can be processed. Given this conventional scenario, the consumer is vulnerable when the credit card is lost or stolen. They are also vulnerable if the merchant or any employee decides to use the credit card number in a fraudulent manner.

 Thus, there is a need for a system that provides customers the ability to
20 efficiently match their financial account information with their UPI, allowing them to purchase goods or services with their credit card or other financial account, without presenting the actual card. The aim of this system is to optimize customer security and privacy interests.

SUMMARY OF THE INVENTION

25 The present invention is for a system and related method for payment of bills, purchases, or other payments which compares a UPI or a merchant/biller's database of subscribers, customers, potential customers, prospects, or accounts receivables, sometimes referred to herein collectively as "customers", either with a consolidated database of financial account information such as credit card account information, or with a plurality of non-
30 consolidated databases of financial account information, or with a combination of the two types. Many types of financial account information may be used to make the payments,

including, but not limited to, credit cards, charge cards, debit cards, smart cards, bank cards, demand deposit accounts such as checking accounts, virtual payment accounts, virtual cash account numbers such as those provided for commercial transactions over the Internet, wire transfer networks, financial electronic data interchange (FEDI), E-check, Automated Clearing House (ACH), payment products from third party, non-bank financial institutions such as CyberCash and TransPoint (MSFDC), stored value tools such as VisaCash and Mondex, and the like.

The system matches the customer's UPI or the customer identification data contained in a merchant, biller or payment processor's database with the financial account information contained in the one or more financial account databases and selects which one or more financial accounts to present when the customer is a holder of more than one financial account.

The financial account or accounts selected are provided to the merchant or biller for inclusion on a commercial communication, such as a payment stub, renewal form, invoice, or other marketing material soliciting payment or subscription. Optionally, the merchant/biller need not know the particular financial account or number being used. For example, a commercial communication may indicate the issuer of the financial account, such as a credit card, and a particular financial account, such as a particular credit card account, for the customer to charge the purchase to, but include the account number only in encrypted form, thus offering security and privacy to the consumer. Many forms of securing information are known and may be used, including but not limited to the use of encryption techniques and record locator techniques.

For example, in a transaction where the financial account utilized is a credit card account, the customer can indicate his approval to use the credit card number provided in encrypted form and thus does not have to provide the information himself when paying by credit card. The merchant/biller collects the invoices or other offers with the customer's indication or authorization of payment from the credit card account and, optionally, submits it to a service bureau which decrypts the credit card account number and processes billing to the selected credit card account. This helps preserve the customer's privacy in his or her credit card and related information.

As shown in Fig. 2, the system of the present invention serves as an

intermediary between a large number of issuers and a large number of merchants. As shown in Fig. 2, issuers provide their account information lists to the central account management and consolidation system of the present invention, which in turn receives customer identification data from merchants, and matches and selects financial account information to provide to 5merchants, as described above.

In some embodiments, the system includes a memory device which stores consolidated multiple financial account information, such as a master financial account list, which includes, for example, credit card account information from multiple credit card issuers. A computer system or other processing unit matches customer identification data from the 10stored consolidated financial account information to a UPI or to a database of a merchant/biller's customer identification data in order to associate a financial account number with a selected member of the customer database. The computer system or processing unit selects one or more specific associated financial account numbers when more than one financial account number matches the selected member of the merchant/biller's customer database. If 15not previously encrypted, the associated financial account number is encrypted and provided to the merchant/biller for inclusion on the customer's commercial communication, such as a bill, payment stub, renewal form or invoice, which is then sent to the customer. After selection and authorization by the customer, the system may also decrypt the encrypted financial account number for processing payment to the merchant/biller from the selected 20financial account of the customer.

Alternatively, in lieu of including a master consolidated database of financial account information, the system may be comprised of a plurality of databases of financial account information either internal or remote, and a mechanism for searching the various databases to locate a customer's financial account information. The various financial account 25information databases may include databases of individual issuers and/or partially consolidated databases containing information from a number of financial account issuers.

A method in accordance with one embodiment of the invention includes the steps of consolidating multiple financial account information lists from multiple financial account issuers into a master financial account list, receiving a UPI or a merchant/biller's customer 30database, and matching information from the master financial account list to the customer's UPI or to the master/biller's database to associate at least one financial account number for

each customer. In accordance with desired selection rules, one or more of the matching financial account number(s) is selected, if more than one financial account number is found for a particular customer. The selected financial account number is encrypted, or may be provided already encrypted in the financial account databases. The encrypted financial account number or numbers are provided to the merchant/biller for inclusion on the merchant/biller's commercial communication to the customer, thus providing the customer with a means for authorizing payment for purchase to the associated financial account number, such as a particular credit card. Payment for the purchase is processed and made to the merchant/biller from the financial account of the authorizing member. Of course, a financial account number can be any unique encrypted identifier, even those including letters as well as numbers.

Alternatively, instead of consolidating multiple financial account information from a number of financial account issuers into a single master financial account database or list, the method may include consolidating some subset of financial account lists and searching a plurality of such lists as well as lists from individual financial account issuers in order to associate at least one financial account number for each customer in the merchant/biller's customer database, or searching a plurality of individual financial account lists made available by different issuers.

In another embodiment, the present invention is directed to a system and method for providing automated payments over a computer network, for example, over the Internet. The system includes an automated payment server which is connected to various financial institutions and which receives and compiles data from those institutions to create files of account information for various customers. When a customer desires to purchase goods from a merchant's web site, or to pay bills, the customer is routed to the payment server, and is presented with the account information as compiled by the payment server. The customer selects one or more of the financial accounts, and the payment server transmits the appropriate financial information to the merchant's payment processor to complete the transaction. In this manner, credit card numbers are not transmitted over the Internet or stored on a merchant's site, but are only transmitted between the payment server and the payment processor, preferably over a secure line.

BRIEF DESCRIPTION OF THE DRAWINGS

15 For a fuller understanding of the invention, reference is made to the following description taken in connection with the accompanying drawings, in which:

Fig. 1 is a block diagram illustrating the problems encountered in matching a large number of financial account issuers to a large number of merchants/billers in an automated payment system;

20 Fig. 2 is a block diagram illustrating the use of the present invention in efficiently matching a large number of financial account issuers to a large number of merchants/billers in an automated payment system;

Fig. 3 is a block diagram of a preferred embodiment of an apparatus for carrying out the automated credit card payment method and system of the present invention;

25 Fig. 4 is a flow chart illustrating the use of the apparatus of Fig. 3;

Fig. 5 is a block diagram of an alternative embodiment of the present invention;

Fig. 6 is a block diagram of an automated payment system used for billers in accordance with one preferred embodiment of the invention;

Fig. 7 is a flow chart illustrating the use of the system of Fig. 6;

30 Fig. 8 is a block diagram of an alternative embodiment of the present invention;

Fig. 9 is a flow chart illustrating the use of the system of Fig. 8;

Figs. 10 and 11 are representations of an interface presented to a customer upon accessing a payment server according to one aspect of the invention; and

Fig. 12 is a block diagram of an embodiment of an apparatus for carrying out the automated credit card payment method and system of the present invention using a bricks-and-mortar terminal and a biometric identifier and/or PIN.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Preferred embodiments of the invention are now described with reference to the drawings. Although many of the drawings and descriptions illustrate the use of the invention with credit card accounts for the sake of simplicity, the invention is in no way meant to be limited to credit card accounts.

Referring to Fig. 3, an automatic payment system 50 according to one embodiment of the present invention is shown. The system 50 may utilize any combination of many types of financial accounts and is described with reference to credit card accounts for simplicity. The system 50 may be operated by a company, such as a service bureau, and includes a database consolidation and sorting subsystem 55, a master credit card database 57, an identifier matching and selecting subsystem 59, and an optional credit card account number encryption subsystem 53.

The automatic payment system 50 is used in conjunction with n number of credit card issuers 60_0 to 60_n . Each of the n credit card issuers 60 maintains on a computer system its own credit card information list 66_0 to 66_n in accordance with one of a number of conventional format types known to those of skill in the art. These credit card information lists 66 typically contain account holder identification data, such as the name and address of each account holder, as well as the associated credit card number, name of financial institution, account information and demographic information pertaining to each card holder. One skilled in the art will recognize that although the preferred embodiments are described with reference to the use of credit cards, other financial account information or devices, including but not limited to smart cards, bank cards, checking accounts, and virtual payment accounts used for Internet and other on-line commercial transactions, may be used instead of or in any combination with credit card accounts.

The automated payment system 50 receives credit card information lists 66 over

a transmission medium 68 from the n credit card issuers 60. This transfer of information over medium 68 may be achieved by many communications methods, including but not limited to modem connections, high speed data lines, the Internet, or the physical transfer of storage media, such as tapes or disks. This transfer is authorized by contractual relationships and may include financial incentives. In order to increase the likelihood of locating customer credit card information, it is preferable to include the credit card account information from as many credit card issuers as possible. The database consolidation and sorting subsystem 55, which may be in the form of a programmed computer system, sorts and consolidates the credit card information 66₀ to 66 _{n} provided by the credit card issuers 60₀ to 60 _{n} , and the sorted and consolidated data is then stored in the master credit card information database 57. This database may reside on a mass storage unit of the computer system. Of course, the processing elements and information storage elements may reside on multiple computing devices to provide for contingencies such as fault tolerance and load balancing.

The automated payment system 50 is used to provide credit card account information to one or more of m number of merchants/billers 70₀ to 70 _{m} . Each of the m merchants/billers may maintain on a computer its own list 76 of customer identification data. These lists 76₀ to 76 _{m} include customer identification data such as names and addresses of customers or additional information, such as social security numbers and demographic information. The automatic payment system 50 receives the customer identification data from a given merchant/biller 70 _{x} , and the matching and selecting subsystem 59 compares the customer identification data supplied by merchants/billers 70 _{x} with the records in the master credit card information database 57 to locate matching credit card holder identification data. The matching and selecting subsystem 59 may be in the form of a preprogrammed computer system which is either the same as the one used for the database consolidation and sorting subsystem 55, or separate therefrom. The process of matching customers from a merchant/biller database to credit card account holders in the matching and selecting subsystem 59 may be performed using conventional matching algorithms as known to those of skill in the art.

If more than one credit card holder identifier matches a given customer (i.e., the customer has more than one credit card), one or more of the matching credit card identifiers is selected or featured by the matching and selecting subsystem 59. This selection

proceeds in accordance with certain selection and presentation rules. As an illustrative example, a simple selection rule is used wherein the selected credit card is the one issued by the issuer having the most credit cards in the database, i.e., the most “popular” or predominant credit card. Alternatively, in one embodiment, the selection is made on a pro rata basis or other algorithm based on the total number of credit card accounts for each issuer in relation to the number of credit card accounts for the other issuers and the total number of credit card accounts in the master credit card database 57. Thus, for example, a credit card issuer which accounts, for example, for 25% of the total number of credit card accounts in the consolidated database, will have its associated credit card account selected 25% of the time for customers 10 who have multiple credit card number accounts including that issuer. Another method of selecting one associated credit card account number from more than one matching associated credit card account is to compare the selected associated credit card account numbers with credit card usage information to determine the customer's primary credit card, based on amount of use, and selecting the customer’s most often used credit card. Yet another method 15 of selecting an account may take into consideration the fees associated with financial transactions and select the financial institution that charges the lowest fees. Alternatively, the selection process may take into account historical data and select the financial institution that yields the best results or success for a particular merchant/biller. Finally, the selection may be made as a result of fees paid by the credit card issuer to receive priority in the selection 20 process.

In alternative embodiments, more than one credit card, or all of the credit cards, may be selected for inclusion, and the customer is given the option of selecting which one of the cards is to be used for making payment. In this embodiment, all matching credit card account numbers may be selected and presented to the customer. The selected credit card 25 accounts may be presented to the customer in a list with a check box, such as in the following form:

Choose the card(s) with which you wish to pay:

- CITIBANK VISA
- DISCOVER
- 30 AMERICAN EXPRESS

In a more preferred embodiment of the present invention, the selected credit card accounts can also be ordered and presented to the user, based on similar criteria as that used by the system to determine the selection of credit cards, *e.g.*, the most popular card in the database, the customer's most often used credit card, the card that charges the lowest fees, or the card whose issuer has paid the highest fee, can be presented above or ahead of other credit cards.

The selected credit card account number or numbers which are to be included on a commercial communication are encrypted by a credit card account number encryption subsystem 53. The particular method of encryption may include a finder number, record locator, some form of high level encryption, or any other encryption technique. While encryption is an element of the preferred embodiment, the method of encryption may be any method which achieves adequate security and the specific method of encryption does not constitute a material element of the system and method set forth herein. Moreover, credit card information may be encrypted and provided in encrypted form from the credit card issuers before being stored in the master credit card information database.

Fig. 4 illustrates the use of encrypted account information of the present invention, and specifically, encrypted credit card information for the sake of simplicity. In one embodiment, for each customer in a merchant/biller's customer identification data database 76, the encrypted credit card account number associated with the customer is provided by merchant/biller 70_x to the customer (step 80) as part of the communication to the customer from merchant/biller 70_x. Alternatively, in a bricks-and-mortar embodiment of the present invention where the bricks-and-mortar merchant does not have a "customer information database," the customer communicates directly to the central database 57 via a payment process interface, *e.g.*, a terminal or computer. At step 90, the customer decides whether to authorize payment by credit card. This authorization step may also include selecting which credit card(s) to use if the customer is presented with more than one. If the customer authorizes such payment and returns the commercial communication to the merchant/biller or other payment processing entity, the encrypted credit card account number is decrypted at step 100. The encrypted number may be sent by the system 50 to the credit card issuer, a payment processor or merchant for decryption and/or payment processing. After decryption the credit card account number is used to process payment to merchant/biller (step 110) and payment is made to the particular merchant/biller, along with any required payments for use of the system

in handling the transaction. If the customer 90 does not authorize payment, steps 100 and 110 are simply not performed.

It should be understood that elements of the system and method of the present invention described herein, such as in Figures 3 and 4, may be modified in keeping with the intended scope of the invention. For example, the consolidated credit card account database has been described as containing account information from multiple credit card account issuers. However, the merchant/biller's customer identification data may alternatively be matched serially against multiple databases, including individual credit card issuers' credit card account databases and/or one or more consolidated database. Each individual or consolidated database represents some number of credit card issuers which is a subset of all the issuers.

Fig. 5 shows an alternative embodiment of an automated payment system 50' according to the present invention. The system 50' of this alternative embodiment includes a serial matching subsystem 59' and a selection/presentation subsystem 59''. The serial matching subsystem compares customer identification data, received over transmission medium 1569 from a merchant or one or more customer databases 76 of a given merchant/biller 70, to a number of credit card databases 66 of a number of issuers 60. The serial matching subsystem may also compare the customer identification data with a consolidated database 58 containing information consolidated from a limited number of issuers 60, in this case, issuers 3 and 4. The serial matching subsystem locates matches of the merchant/biller's customer identification data with account holder identification data contained in the individual and partially consolidated databases 66 and 58, as discussed above. Once a set of matching credit card account numbers is located, the selection subsystem 59'' selects one or more of the account numbers, in accordance with the selection rules discussed above.

Referring now to Fig. 6, therein is shown a block diagram of an embodiment of the automated credit card payment system of the present invention as applied to merchant/billers. In this arrangement, multiple merchant/billers 150 use a fulfillment house 152 and a service bureau 154 employing the system of the present invention to deal with multiple credit card account databases 156, one or more of which may be partially consolidated databases as explained above. More than one fulfillment house 152 may be utilized to serve the various merchant/billers and/or groups of merchant/billers, or one fulfillment house 152 may be used for each biller 150. Merchant/billers 150 provide the fulfillment house 152 with

each of their customer files 158 and outside lists 160 (e.g., lists of prospective customers). The service bureau 154 uses the system of the present invention to match the names on the merchant/billers' customer files 158 with associated financial account information. This information, including credit card information, is consolidated by the service bureau 154 from multiple credit card issuers 156 and is stored in a master credit card file. Alternatively, this credit card information can be accessed serially from databases of the multiple credit card issuers.

After matching the merchant/billers' customer files 158 and outside lists 160 with associated financial account information, the service bureau encrypts the matching credit card account numbers (block 162) and provides them to the fulfillment house 152. The use of the located credit card information is shown in the flow chart of Fig. 7, where fulfillment house 152 uses the encrypted credit card account information in marketing, billing and/or renewal efforts (step 164), such as by placing encrypted credit card account numbers on commercial communications. At step 165, customers authorize the use of their credit card, and optionally select which credit card to use if more than one is presented to the customer.

When customers place orders using the encrypted credit card account information on the commercial communication, the orders are collected and the encrypted number entered and consolidated into a consolidated order file (step 166). The encrypted account numbers in the consolidated order file are then decrypted (step 170) and payments are processed (step 172).

Referring now to Figs. 8 and 9, there is shown another embodiment of the present invention. In this embodiment, the system 200 is designed for use over a computer network, for example, over the Internet, a LAN, WAN, or the like. The system 200 includes an automated payment server 202 that includes a processing unit 204 and a customer database 206 maintained by the processing unit, and is similar in many respects to the automated payment system 50 described above. The database combines account information from various financial institutions, as well as bill information from various billers.

The automated payment server 202 connects to a plurality of customers at respective terminals 208, and interacts with those customers via a suitable customer interface 210 (only one terminal is shown schematically in FIG. 8). The customer interface can be a basic application used to select payment options, a method of viewing bills from various

billers, and/or a full-service interface that combines those functions and allows the customer to re-configure the account. It will be apparent to those skilled in the art that various forms of interface may be employed.

The automated payment server 202 further connects to one or more merchant sites 212 over one or more communication lines 214. Preferably, at least one of the lines 214 is a secure line for transmission of payment information, as is described in greater detail below.

The automated payment server 202 is connected to various financial institutions 220 and to various billers 222. The automated payment system 202 receives account information, including updated account information, over a transmission medium from the financial institutions, and receives billing information from the various billers, as described above in connection with the automated payment server 50. For example, various utilities may transmit bills electronically to their customers via the payment server 202. An automated account information merge/purge subsystem 224 and an automated bill information merge/purge subsystem 226, which may be in the form of programmed computer systems, sort and consolidate the account and bill information provided by the financial institutions and billers, and the sorted and consolidated data is then stored in the customer database 206 for subsequent access, as is described in greater detail below.

The customer terminals 208 can take many different forms, and can access the automated payment server 202 in many different ways. For example, the customer may transmit purchase requests via a brick-and-mortar terminal, E-mail, or over the Internet by clicking on a banner on a web site, through interactive television, WebTV®, over the telephone, by direct mail, or in any other suitable manner. In one embodiment, the merchant site 212 may post a banner indicating that payment for a transaction may be conducted through the automated payment server 202. The customer can then click on the banner and be directed to the automated payment server, as is described in greater detail below.

The customer interface 210 is preferably a suitable interface that allows the automated payment server 202 to simultaneously communicate with multiple customers over the Internet or other computer network.

Referring now to Fig. 9, the operation of the automated payment server 202 is described in more detail. Operation begins at step 300, with a customer beginning the

transaction by communicating with a merchant 212 and either placing an order or requesting to pay a bill for goods or services. In one embodiment, the merchant site presents the customer with a banner having an embedded URL of the automated payment server 202, or alternatively the merchant site can automatically direct the customer to the automated payment server when the customer places an order. At step 302, the customer is linked to the automated payment server 202, and at step 303 the server determines whether the customer is registered with the server. If the customer is not registered, operation proceeds to step 304, and the customer registers with the payment server. Registration can be conducted over the computer network, over the telephone, through the mail, or in any other suitable manner, and involves receiving identifying information from the customer to verify the identity of the customer for all subsequent transactions. For example, the customer may provide their name, address, etc., along with their mother's maiden name, a social security number, or the like. The customer may also provide biometric information, *e.g.*, fingerprint sample, handwriting sample, retina scan, or voice recording/pattern. Once the customer's identity has been verified, a password is selected for the customer (either chosen by the customer or randomly assigned by the payment server), as is well known in the art.

If the customer is already registered with the payment server 202, the customer inputs his or her user name and password at step 303, and after authentication or verification, the customer is allowed to continue with the payment transaction.

The merchant 212 transmits order and/or payment data to the payment server 202, either automatically or after being prompted by the payment server, at step 305. The data preferably identifies the customer, for example by including order ID data and/or a customer UPI, which is also transmitted to the payment server when the customer accesses the payment server. Alternatively, the merchant site may transmit the customer's name or any other identifying data to allow the payment server to associate the customer with the particular order or payment request.

The customer's UPI or other identifying information is associated with the customer's financial account(s). The UPI can be in the form of a name, password, PIN, ID number, or other unique identifier. Alternatively, the UPI can take the form of a fingerprint, retina scan, voice pattern, handwriting sample, or other unique "biometric" identifier. These biometric identifiers, in some cases, can be used in conjunction with a password or PIN. The

recording, capturing, and storing of unique biometric identifiers such as retina scans, iris scans, voice patterns, digital handwriting samples or digitally scanned fingerprints are described in U.S. Patent Nos. 6,047,281; 6,038,334 and 5,991,408, the disclosures of which are incorporated herein by reference. In one possible embodiment of the invention, the customer's UPI is recorded and/or authenticated using prior art devices, such as digital scanners, cameras or recorders, attached to the consumer's computer or located at a bricks-and-mortar or other merchant terminal as exemplified in Fig. 12.

Once the payment server has associated the customer with the order or payment request, operation proceeds to step 306, and the payment server accesses the customer database to retrieve the customer's account information, which as described above is in the form of various credit cards, debit cards, smart cards, bank cards, demand deposit accounts such as checking accounts, virtual payment accounts, wire transfer networks, financial electronic data interchange (FEDI), Echeck, Automated Clearing House (ACH), payment products from third party, non-bank financial institutions such as CyberCash and TransPoint (MSFDC), stored value tools such as VisaCash and Mondex, and the like. Then, at step 308, the payment server 202 presents the customer account information to the customer (Fig. 10). The account information identifies the various financial to the customer, without transmitting entire account numbers to the customer. For example, some identifying information is transmitted, such as the name of the credit card, the last several digits of a credit card, or the like (e.g., "AmEx 206543"). The account information may include, in addition to identifying the various credit cards and the like, available balance information, date of the last update to that account, date of last payment, credit limit, transaction detail, and the like.

At step 310, the customer selects one or more payment options, and that selection (or selections) is transmitted to the payment server via the interface 210. Thus, the actual account numbers are not transmitted between the payment server and the customer.

The customer may choose to split a payment between two or more financial accounts, for example, two or more credit cards. In addition, the payment server can present the accounts to the customer in some specific order, as defined by the customer, the financial institutions, particular merchants, account usage, available balances, interest rates, and the like.

In one embodiment, the payment server 202 presents the customer only with

appropriate payment options. For example, if the purchase amount is \$100, and the customer's checking account has a balance less than \$100, the payment server preferably does not provide that as an option to the customer. Alternatively, the checking account may be presented to the customer, but in a different color or font to indicate to the customer that such account is not suitable for the particular transaction, but can be used in connection with another payment option to complete the transaction.

At step 312, the payment server 202 transmits a request for authorization to the payment processor of the merchant site 212, which includes the payment option selected by the customer. At step 314, the customer interface determines whether the payment option is acceptable. For example, the customer may have selected a credit card that is not accepted by the particular merchant. If so, operation proceeds to step 316, and the customer is informed that the authorization failed. Operation then flows back to step 308, to allow the customer to select another payment option.

If the payment option is acceptable at step 314, operation proceeds to step 318, and the customer is notified that the transaction has been approved. Then, at step 320, the payment server 202 transmits the approved order or Approval to the merchant site or to the merchant's payment processor 212, preferably over a secure line, and the merchant fills the order by interacting with the customer 208. For example, the merchant site may request shipping information if they do not already have it or other required information to complete the transaction. Then, at step 322, the payment processor accesses the appropriate financial institution and transmits the payment information, so that the customer's account is debited and the merchant's account is credited.

It will be apparent to those skilled in the art that the above steps may also be carried out over a telephone network that allows for interactivity, such as those systems offering voice recognition and/or dual tone multi-frequency (DTMF) tones. As is well known in the art, the customer may enter a user ID and password by pressing the appropriate keys on the telephone, with the payment server including the appropriate, well-known hardware to interpret the DTMF tones to determine the corresponding numbers entered by the customer. Thus, a customer may dial a telephone number, listen to a list of available goods, services and/or bills, and select one or more of the goods, services and/or bills by pressing appropriate keys on the telephone. The payment server, through a well-known interactive system such as

interactive voice response (IVR) or the like, then prompts the customer to enter identification data, such as a user name and PIN number, or the like. Once the identity of the customer is verified, the payment server may then present the customer with a list of credit cards that may be used to complete a transaction. For example, the IVR software may read "Press 1 to select your Visa account, press 2 to select American Express," or the like. The customer may simply press the corresponding key on the telephone to signal the payment server of the customer's choice. The remainder of the process is the same as the computer network version described above. Thus, in this manner the payment server 202 is available to customers over a telephone network.

10 Alternatively, the present invention may be implemented through the mail, by the customer returning an order form sent through regular mail and/or electronic mail. In this manner, the payment server sends a preprinted order form to potential customers, listing various goods, services and/or bills available, and also listing that particular customer's financial accounts as compiled by the customer database 206. The customer selects one or
15 more of the goods, services and/or bills, selects a financial account for payment from the customer-specific list printed on the form, and returns the order form to the payment server 202. An operator at the payment server then enters the data, or in the case of electronic transfer such as email, the data is uploaded. The payment server forwards the data to the appropriate merchant. If the payment option selected by the customer is not appropriate (e.g.,
20 the merchant does not accept that type of payment or the available balance is too low), the customer is notified, either through the mail (electronic or regular) or via telephone, and may select another payment option. Once a suitable payment option is selected, the remainder of the transaction is completed along the lines of the computer network version described above.

In an alternative embodiment, the customer who receives the order form or bill
25 may call a telephone number provided on the form and complete the transaction over the telephone, in the same manner as described above.

In another embodiment, the customer at terminal 208 may access the payment server 202 directly without initially accessing a merchant's site. The customer then may be presented with outstanding bills, as compiled by the automated bill information merge/purge
30 subsystem 226 (Fig. 11). The customer may select one or more of the bills to be paid, and is then presented with the account information, similar to the process described above with

respect to Fig. 9.

It will be apparent that the system and method of the present invention allow payment transactions to be performed over a computer network without requiring any credit card numbers or the like to be transmitted directly between the customer 208 and merchant 5212, or between the customer 208 and the payment server 202. Thus, no account information passes over a public network such as the Internet. The account information is transmitted over secure lines between the financial institutions and the payment server 202, and between the payment server and the merchant's payment processor or the merchant's site. In addition, multiple merchants do not need to maintain a database of account numbers, as such information 10 is maintained at the payment server 202. Maintaining the database at one location rather than at each individual merchant further reduces the likelihood of fraud.

Referring to Fig. 12, an automatic payment system 50 is shown according to an embodiment that implements use of biometric identifiers and/or PINs. A biometric identifier and/or PIN is collected at a bricks-and-mortar terminal. A bricks-and-mortar terminal may 15 include a computer, digital camera, scanner, recorder or other device capable of capturing such information. The automatic payment system 50 receives the biometric identifier and/or PIN from the bricks-and-mortar terminals 84_x, and the matching and selecting subsystem 59 compares the biometric identifier and/or PIN 88_x with the records in the master credit card information database 57 to locate matching credit card holder identification data. The matching 20 and selecting subsystem 59 may be in the form of a preprogrammed computer system which is either the same as the one used for the database consolidation and sorting subsystem 55, or separate therefrom. The process of matching customers from a merchant/biller database to credit card account holders in the matching and selecting subsystem 59 may be performed using conventional matching algorithms as known to those of skill in the art. If a match is 25 found in the master credit card database 57, then the PIN is validated.

As can be understood from the above description of the present invention, the present invention provides a number of benefits to customers (such as credit card users), financial institutions, merchants and billers. Benefits for the financial institutions include reduced fraud, more credit card usage, higher retention rates, and increased fee income. 30 Benefits for the customer include convenience, privacy, and efficiency. Benefits to the merchant/billers are reduced fraud and theft, higher retention rates, less bad debt, savings on

mailing expense, and better customer relationships.

The system and method of the present invention may also be used in conjunction with a targeted marketing or coupon plan in which purchasing behavior can be identified and recorded by the payment server. In one possible embodiment, consumers with financial accounts (including credit card accounts) on the payment server can acquiesce in having their purchasing behavior tracked and provided to a wide variety of businesses and industries. These business and industries can then preferentially target various consumers for discounts, coupons, or other marketing deals based on their past purchases.

Another benefit provided by the present invention is the security and privacy for consumers. Therefore, in accordance with the preferred embodiment of the invention herein, a centralized organization or company is the only party, aside from the financial institutions with relationships with the consumers, as well as the consumers themselves, that has access to the specific financial account information. It should be understood that the functions performed by the central organization may actually be divided between separate entities. For example, one entity may perform processing, while another entity performs encryption/decryption. As described above, only encrypted account information is provided to the merchants/billers; however, it is within the scope of the present invention to provide a system in which accounts are provided to merchants/billers directly, and the merchant/biller or other company encrypts such account information for use in its billing materials. In such a case, once the merchant/biller receives the customer's approval for charging a particular account, it can proceed to decrypt and process the payment from the financial institution directly.

Many other user functions known in the art can be implemented such as the ability to allow a user to modify his user registration information.

While several forms of the invention have been described, it will be apparent to those skilled in the art that various modifications and improvements may be made without departing from the spirit and scope of the invention.

WHAT IS CLAIMED IS:

1. A method for facilitating payment from a customer's financial account to a merchant/biller or a payment processor associated with a merchant/biller, comprising the steps of:

compiling in a memory financial account information for at least one customer from a plurality of financial institutions;

receiving and storing transaction information relating to a particular customer;

retrieving from the memory the financial account information for the customer;

presenting the financial account information to the customer;

receiving and storing a selection by the customer of at least one of the financial accounts; and

providing the selected financial account(s) information either to the merchant/biller or to a payment processor associated with the merchant/biller.

1 2. The method of claim 1, wherein said financial account corresponds to at
2 least one of a credit card, charge card, debit card, smart card, bank card, demand deposit account,
3 checking account, virtual payment account, virtual cash account, wire transfer networks, financial
4 electronic data interchange (FEDI), Echeck, Automated Clearing House (ACH), and stored value
5 tools.

1 3. The method of claim 1, further comprising the step of consolidating at
2 least two of said plurality of financial account information databases into a single consolidated
3 financial account information database and wherein said retrieving step includes the step of
4 searching said consolidated database.

1 4. The method of claim 1, further comprising the steps of selecting a subset
2 of one or more financial accounts from among a plurality of customer financial accounts, and
3 presenting the subset to the customer.

1 5. The method of claim 4, wherein the subset of accounts includes financial
2 accounts acceptable to the merchant/biller.

1 6. The method of claim 1, further comprising the step of dividing payment
2 for a single transaction among more than one financial account if more than one financial account
3 is selected.

1 7. The method of claim 1, further comprising the step of selecting the order
2 in which one or more financial accounts are presented to the customer before presenting the
3 financial account information to the customer.

1 8. The method of claim 1, further comprising the steps of encrypting said
2 selected customer financial account information prior to providing it to said merchant/biller, or
3 payment processor, and encrypting or truncating the financial account information before it is
4 presented to the customer.

1 9. The method of claim 1, further comprising the step of updating said
2 financial account information from at least one of said plurality of financial institutions.

1 10. The method of claim 1, further comprising the steps of determining
2 whether a customer is a registered customer; and
3 registering a customer if the customer is not yet registered.

1 11. The method of claim 10, wherein the step of registering a customer further
2 includes capturing a PIN and a biometric measurement of the customer.

12. The method of claim 11, wherein the biometric measurement includes voice patterns, fingerprints, retina scans, or handwriting samples.

13. The method of claim 11, further comprising the step of comparing the PIN, biometric measurement, or both, against a respective stored database of PINs or biometric measurements.

14. The method of claim 1, further comprising the step of comparing a transaction value from the transaction information to an available balance value from the financial account information.

15. The method of claim 14, further comprising the step of presenting to customers only those financial accounts with an individual or combined available fund balance equal to or greater than the transaction value.

16. A method for facilitating payment from a customer's financial account for a bill selected from a plurality of bills presented to the customer, the method comprising the following steps:

compiling in a memory financial account information for at least one customer from a plurality of financial institutions;

presenting the customer with bill information for each of a plurality of bills;

receiving selection information from the customer specifying a particular selected bill which is to be paid;

retrieving from the memory the financial account information for the customer;

presenting the financial account information to the customer; and

receiving selection information from the customer specifying a particular account to be used to pay the selected bill.

1 17. The method of claim 16, wherein said financial account corresponds to
2 at least one of a credit card, charge card, debit card, smart card, bank card, demand deposit
3 account, checking account, virtual payment account, virtual cash account, wire transfer networks,
4 financial electronic data interchange (FEDI), Echeck, Automated Clearing House (ACH), and
5 stored value tools.

1 18. The method of claim 16, further comprising the step of consolidating at
2 least two of said plurality of financial account information databases into a single consolidated
3 financial account information database and wherein said retrieving step includes the step of
4 searching said consolidated database.

1 19. The method of claim 16, further comprising the steps of selecting a subset
2 of one or more financial accounts from among a plurality of customer financial accounts, and
3 presenting the subset to the customer.

1 20. The method of claim 19, wherein the subset of accounts includes financial
2 accounts acceptable to the merchant/biller.

1 21. The method of claim 16, further comprising the step of dividing payment
2 for a single transaction among more than one financial account if more than one financial account
3 is selected.

1 22. The method of claim 16, further comprising the step of selecting the order
2 in which one or more financial accounts are presented to the customer before presenting the
3 financial account information to the customer.

1 23. The method of claim 16, further comprising the steps of encrypting said
2 selected customer financial account information prior to providing it to said merchant/biller, or
3 payment processor, and encrypting or truncating the financial account information before it is
4 presented to the customer.

24. The method of claim 16, further comprising the step of updating said financial account information from at least one of said plurality of financial institutions.

25. The method of claim 16, further comprising the steps of determining whether a customer is a registered customer; and registering a customer if the customer is not yet registered.

26. The method of claim 25, wherein the step of registering a customer further includes capturing a PIN, an IP address or a biometric measurement of the customer.

27. The method of claim 26, wherein the biometric measurement includes voice patterns, fingerprints, retina scans, or handwriting samples.

28. The method of claim 26, further comprising the step of comparing at least one of the PIN, IP address, biometric measurement, against a respective stored database of PINs, IP addresses or biometric measurements.

29. The method of claim 16, further comprising the step of comparing a transaction value from the transaction information to an available balance value from the financial account information.

30. The method of claim 29, further comprising the step of presenting to customers only those financial accounts with an individual or combined available fund balance equal to or greater than the transaction value.

1 31. A method for facilitating payment from a customer's financial account to
2 a merchant/biller or a payment processor associated with a merchant biller over a computer
3 network, comprising the steps of:

4 compiling in a memory at a payment server financial account information
5 for at least one customer, said information being received from a plurality of financial
6 institutions;

7 receiving over the computer network transaction information at the
8 payment server relating to a particular customer and storing the transaction information;

9 retrieving from the memory the financial account information for the
10 customer;

11 transmitting the financial account information over the computer network
12 to the customer;

13 receiving over the computer network a selection by the customer of one
14 or more of the financial accounts and storing the selection; and

15 transmitting the selected financial account information over the computer
16 network to said merchant/biller or a payment processor associated with the merchant/biller.

17 32. The method of claim 31, wherein said financial account corresponds to
18 at least one of a credit card, charge card, debit card, smart card, bank card, demand deposit
19 account, checking account, virtual payment account, virtual cash account, wire transfer networks,
20 financial electronic data interchange (FEDI), Echeck, Automated Clearing House (ACH), and
21 stored value tools.

22 33. The method of claim 31, further comprising the step of consolidating at
23 least two of said plurality of financial account information databases into a single consolidated
24 financial account information database and wherein said retrieving step includes the step of
25 searching said consolidated database.

1 34. The method of claim 31, further comprising the steps of selecting a subset
2 of one or more financial accounts from among a plurality of customer financial accounts, and
3 presenting the subset to the customer.

1 35. The method of claim 34, wherein the subset of accounts includes financial
2 accounts acceptable to the merchant/biller.

1 36. The method of claim 31, further comprising the step of dividing payment
2 for a single transaction among more than one financial account if more than one financial account
3 is selected.

1 37. The method of claim 31, further comprising the step of selecting the order
2 in which one or more financial accounts are presented to the customer before presenting the
3 financial account information to the customer.

1 38. The method of claim 31, further comprising the steps of encrypting said
2 selected customer financial account information prior to providing it to said merchant/biller, or
3 payment processor, and encrypting or truncating the financial account information before it is
4 presented to the customer.

1 39. The method of claim 31, further comprising the step of updating said
2 financial account information from at least one of said plurality of financial institutions.

1 40. The method of claim 31, further comprising the steps of determining
2 whether a customer is a registered customer; and
3 registering a customer if the customer is not yet registered.

1 41. The method of claim 40, wherein the step of registering a customer further
2 includes capturing a PIN, IP address or a biometric measurement of the customer.

1 42. The method of claim 41, wherein the biometric measurement includes
2 voice patterns, fingerprints, retina scans, or handwriting samples.

1 43. The method of claim 41, further comprising the step of comparing at least
2 one of the PIN, IP address, and biometric measurement, against a respective stored database of
3 PINs, IP addresses or biometric measurements.

1 44. The method of claim 31, further comprising the step of comparing a
2 transaction value from the transaction information to an available balance value from the
3 financial account information.

1 45. The method of claim 44, further comprising the step of presenting to
2 customers only those financial accounts with an individual or combined available fund balance
3 equal to or greater than the transaction value.

46. A method for facilitating payment from a customer's financial account to a merchant/biller or a payment processor associated with a merchant biller, comprising the steps of:

compiling in a memory at a payment server financial account information for at least one customer, said information being received from a plurality of financial institutions;

receiving transaction information relating to a particular customer;

transmitting said transaction information to the payment server and storing the transaction information;

retrieving from the memory the financial account information for the customer;

displaying the financial account information on an interface;

receiving a selection by the customer of at least one of the financial accounts and storing the selection; and

transmitting the selected financial account(s) information either to the merchant/biller or to a payment processor associated with the merchant/biller.

47. The method of claim 46, wherein said financial account corresponds to at least one of a credit card, charge card, debit card, smart card, bank card, demand deposit account, checking account, virtual payment account, virtual cash account, wire transfer networks, financial electronic data interchange (FEDI), Echeck, Automated Clearing House (ACH), and stored value tools.

48. The method of claim 46, further comprising the step of consolidating at least two of said plurality of financial account information databases into a single consolidated financial account information database and wherein said retrieving step includes the step of searching said consolidated database.

49. The method of claim 46, further comprising the steps of selecting a subset of one or more financial accounts from among a plurality of customer financial accounts, and presenting the subset to the customer.

50. The method of claim 49, wherein the subset of accounts includes financial accounts acceptable to the merchant/biller.

51. The method of claim 46, further comprising the step of dividing payment for a single transaction among more than one financial account if more than one financial account is selected.

52. The method of claim 46, further comprising the step of selecting the order in which one or more financial accounts are presented to the customer before presenting the financial account information to the customer.

53. The method of claim 46, further comprising the steps of encrypting said selected customer financial account information prior to providing it to said merchant/biller, or payment processor, and encrypting or truncating the financial account information before it is presented to the customer.

54. The method of claim 46, further comprising the step of updating said financial account information from at least one of said plurality of financial institutions.

55. The method of claim 46, further comprising the steps of determining whether a customer is a registered customer; and
registering a customer if the customer is not yet registered.

56. The method of claim 55, wherein the step of registering a customer further includes capturing a PIN, IP address or a biometric measurement of the customer.

57. The method of claim 56, wherein the biometric measurement includes voice patterns, fingerprints, retina scans, or handwriting samples.

58. The method of claim 56, further comprising the step of comparing at least one of the PIN, IP address and biometric measurement, against a respective stored database of PINs, IP addresses or biometric measurements.

59. The method of claim 46, further comprising the step of comparing a transaction value from the transaction information to an available balance value from the financial account information.

60. The method of claim 59, further comprising the step of presenting to customers only those financial accounts with an individual or combined available fund balance equal to or greater than the transaction value.

61. The method of claim 46, wherein the interface includes a terminal, smart terminal, smart box, keypad, LCD display, cardswipe device or touchpad.

62. The method of claim 46, wherein only those financial accounts acceptable to the merchant/biller are displayed on the interface.

63. A method for facilitating direct bill payment by a customer, comprising the steps of:

receiving and storing billing information from a merchant/biller or merchant payment processor relating to a particular customer;

retrieving from a customer database financial account information for the customer compiled from a plurality of financial institutions;

presenting to the customer a bill payment interface with one or more of the customer's financial accounts;

receiving and storing a selection by the customer of at least one of the financial accounts for payment of the bill; and

providing the selected financial account(s) information either to the merchant/biller or to a payment processor associated with the merchant/biller.

64. The method of claim 63, wherein said financial account corresponds to at least one of a credit card, charge card, debit card, smart card, bank card, demand deposit account, checking account, virtual payment account, virtual cash account, wire transfer networks, financial electronic data interchange (FEDI), Echeck, Automated Clearing House (ACH), and stored value tools.

65. The method of claim 63, further comprising the step of consolidating at least two of said plurality of financial account information databases into a single consolidated financial account information database and wherein said retrieving step includes the step of searching said consolidated database.

66. The method of claim 63, further comprising the steps of selecting a subset of one or more financial accounts from among a plurality of customer financial accounts, and presenting the subset to the customer.

67. The method of claim 66, wherein the subset of accounts includes financial accounts acceptable to the merchant/biller.

68. The method of claim 63, further comprising the step of dividing payment for a single transaction among more than one financial account if more than one financial account is selected.

69. The method of claim 63, further comprising the step of selecting the order in which one or more financial accounts are presented to the customer before presenting the financial account information to the customer.

70. The method of claim 63, further comprising the steps of encrypting said selected customer financial account information prior to providing it to said merchant/biller, or payment processor, and encrypting or truncating the financial account information before it is presented to the customer.

71. The method of claim 63, further comprising the step of updating said financial account information from at least one of said plurality of financial institutions.

72. The method of claim 63, further comprising the steps of determining whether a customer is a registered customer; and
registering a customer if the customer is not yet registered.

73. The method of claim 72, wherein the step of registering a customer further includes capturing a PIN, IP address or a biometric measurement of the customer.

74. The method of claim 73, wherein the biometric measurement includes voice patterns, fingerprints, retina scans, or handwriting samples.

75. The method of claim 73, further comprising the step of comparing at least one of the PIN, IP address or biometric measurement, against a respective stored database of PINs, IP addresses or biometric measurements.

1 76. The method of claim 63, further comprising the step of comparing a
2 transaction value from the transaction information to an available balance value from the
3 financial account information.

1 77. The method of claim 76, further comprising the step of presenting to
2 customers only those financial accounts with an individual or combined available fund balance
3 equal to or greater than the transaction value.

1 78. An apparatus for facilitating payment from a customer's financial account
2 to a merchant/biller or a payment processor associated with a merchant/biller, comprising:

3 a processor; and

4 a memory storing processing instructions for controlling the processor, the
5 processor operative with the processing instructions to:

6 compile in a memory financial account information for at least one
7 customer from a plurality of financial institutions;

8 receive and storing transaction information relating to a particular
9 customer;

0 retrieve from the memory the financial account information for the
1 customer;

2 present the financial account information to the customer;

3 receive and store a selection by the customer of at least one of the financial
4 accounts; and

5 provide the selected financial account(s) information either to the
6 merchant/biller or to a payment processor associated with the merchant/biller.

1 79. The system of claim 78, wherein said financial account corresponds to at
2 least one of a credit card, charge card, debit card, smart card, bank card, demand deposit account,
3 checking account, virtual payment account, virtual cash account, wire transfer networks, financial
4 electronic data interchange (FEDI), Echeck, Automated Clearing House (ACH), and stored value
5 tools.

1 80. The system of claim 78, wherein the processor is operative to consolidate
2 at least two of said plurality of financial account information databases into a single consolidated
3 financial account information database.

1 81. The system of claim 78, wherein the processor is operative to select a
2 subset of one or more financial accounts from among a plurality of customer financial accounts,
3 and to present the subset to the customer.

1 82. The system of claim 78, wherein the processor is operative to select a
2 subset of accounts that includes financial accounts acceptable to the merchant/biller.

1 83. The system of claim 78, wherein the processor is operative to divide a
2 payment for a single transaction among more than one financial account if more than one
3 financial account is selected.

1 84. The system of claim 78, wherein the processor is operative to select the
2 order in which one or more financial accounts are presented to the customer before presenting
3 the financial account information to the customer.

1 85. The system of claim 78, wherein the processor is operative to encrypt said
2 selected customer financial account information prior to providing it to said merchant/biller or
3 to said payment processor, and to encrypt or truncate the financial account information before
4 it is presented to the customer.

1 86. The system of claim 78, wherein the processor is operative to update said
2 financial account information from at least one of said plurality of financial institutions.

1 87. The system of claim 78, wherein the processor is operative to determine
2 whether a customer is a registered customer, and to register the customer if the customer is not
3 yet registered.

1 88. The system of claim 87, wherein the processor is operative to capture a
2 PIN, IP address or a biometric measurement of the customer as part of the registration.

1 89. The system of claim 88, wherein the biometric information includes voice
2 patterns, fingerprints, retina scans, or handwriting samples.

1 90. The system of claim 88, wherein the processor is operative to compare at
2 least one of the PIN, IP address and biometric measurement, against a respective stored database
3 of PINs, IP addresses or biometric measurements.

1 91. The system of claim 78, wherein the processor is operative to compare a
2 transaction value from the transaction information to an available balance value from the
3 financial account information.

1 92. The system of claim 91, wherein the processor is operative to present to
2 customers only those financial accounts with an individual or combined available fund balance
3 equal to or greater than the transaction value.

1 93. An apparatus for facilitating payment from a customer's financial account
2 for a bill selected from a plurality of bills presented to the customer, comprising:

3 a processor; and

4 a memory storing processing instructions for controlling the processor, the
5 processor operative with the processing instructions to:

6 compile in a memory financial account information for at least one
7 customer from a plurality of financial institutions;

8 present the customer with bill information for each of a plurality of bills;

9 receive selection information from the customer specifying a particular
0 selected bill which is to be paid;

1 retrieve from the memory the financial account information for the
2 customer;

3 present the financial account information to the customer; and

4 receive selection information from the customer specifying a particular
5 account to be used to pay the selected bill.

94. An apparatus for facilitating payment from a customer's financial account to a merchant/biller or a payment processor associated with a merchant/biller over a computer network, comprising:

a processor; and

a memory storing processing instructions for controlling the processor, the processor operative with the processing instructions to:

compile in a memory at a payment server financial account information for at least one customer, said information being received from a plurality of financial institutions;

receive over the computer network transaction information at the payment server relating to a particular customer and storing the transaction information;

retrieve from the memory the financial account information for the customer;

transmit the financial account information over the computer network to the customer;

receive over the computer network a selection by the customer of one or more of the financial accounts and storing the selection; and

transmit the selected financial account information over the computer network to said merchant/biller or a payment processor associated with the merchant/biller.

1 95. An apparatus for facilitating payment from a customer's financial account
2 to a merchant/biller or a payment processor associated with a merchant biller, comprising:

3 a processor; and

4 a memory storing processing instructions for controlling the processor, the
5 processor operative with the processing instructions to:

6 compile in a memory at a payment server financial account information
7 for at least one customer, said information being received from a plurality of financial
8 institutions;

9 receive transaction information relating to a particular customer;

0 transmit said transaction information to the payment server and storing the
1 transaction information;

2 retrieve from the memory the financial account information for the
3 customer;

4 display the financial account information on an interface;

5 receive a selection by the customer of at least one of the financial accounts
6 and storing the selection; and

7 transmit the selected financial account(s) information either to the
8 merchant/biller or to a payment processor associated with the merchant/biller.

1 96. An apparatus for facilitating direct bill payment by a customer,
2 comprising:

3 a processor; and

4 a memory storing processing instructions for controlling the processor, the
5 processor operative with the processing instructions to:

6 receive and store billing information from a merchant/biller or merchant
7 payment processor relating to a particular customer;

8 retrieve from a customer database financial account information for the
9 customer compiled from a plurality of financial institutions;

0 present to the customer a bill payment interface with one or more of the
1 customer's financial accounts;

receive and store a selection by the customer of at least one of the financial accounts for payment of the bill; and

provide the selected financial account(s) information either to the merchant/biller or to a payment processor associated with the merchant/biller. --.

FIG. 1

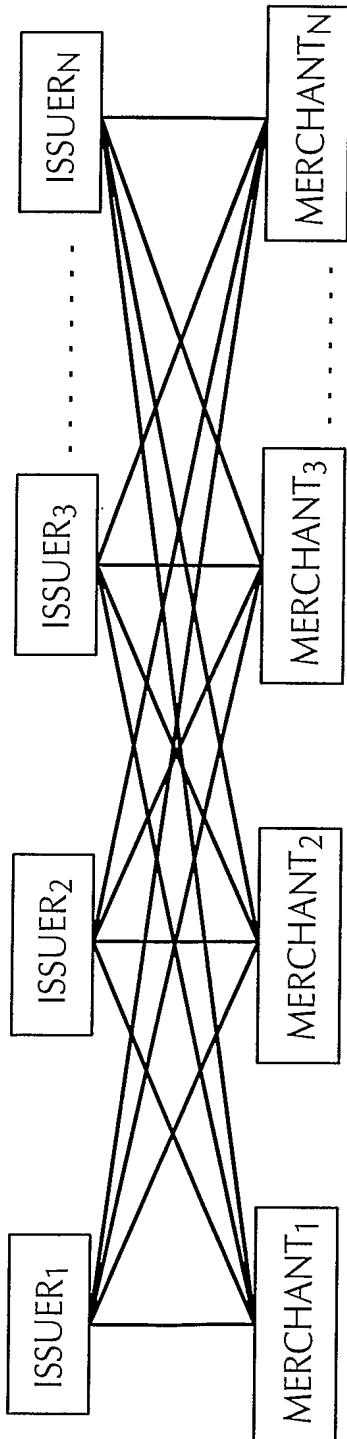


FIG. 2

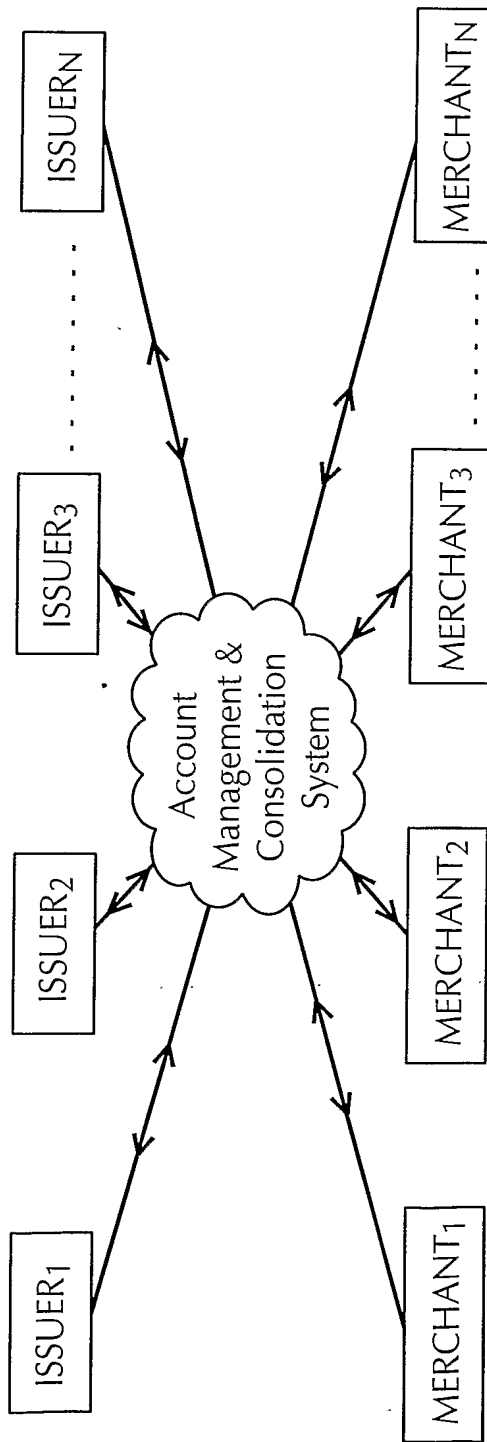
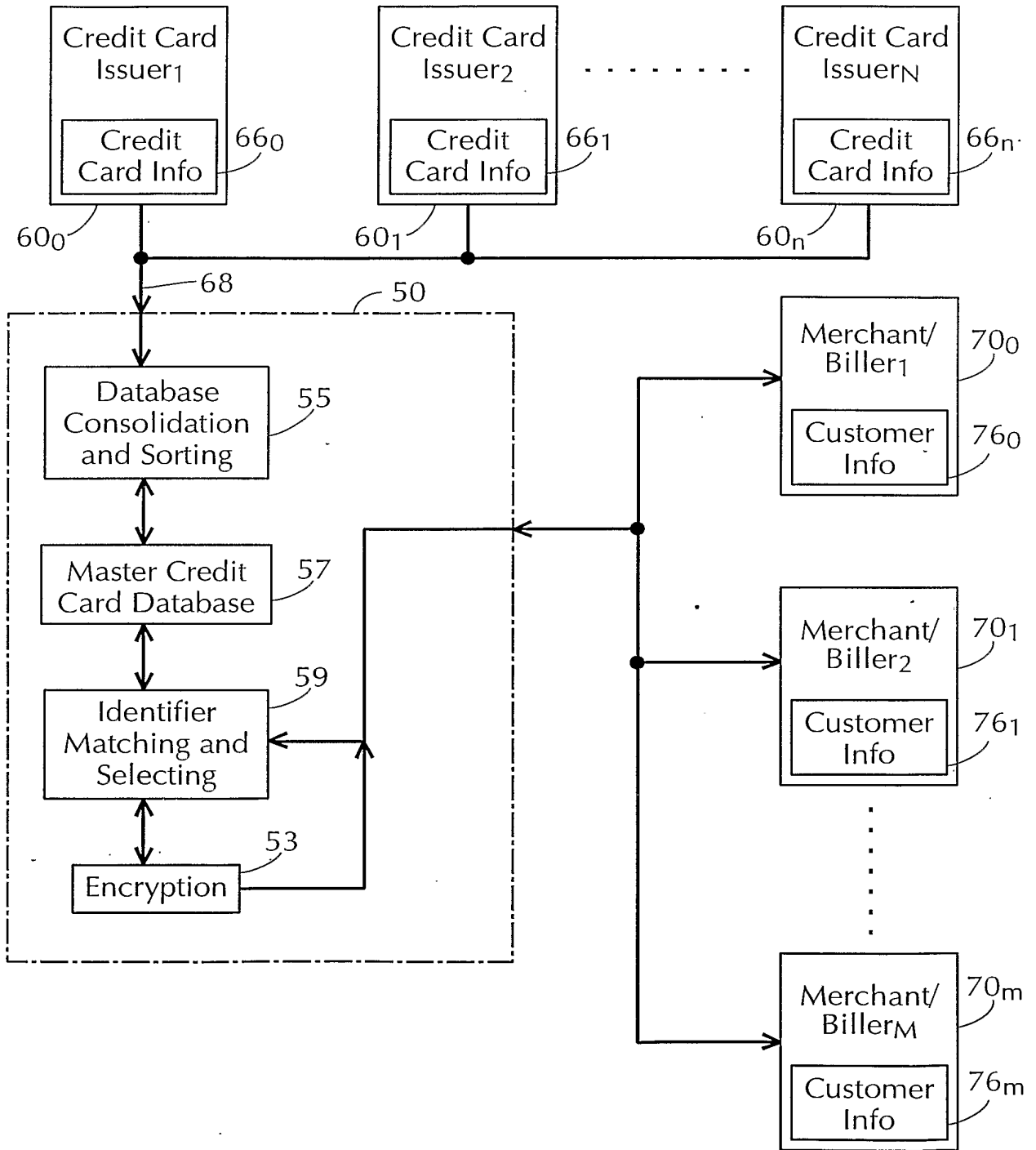


FIG. 3



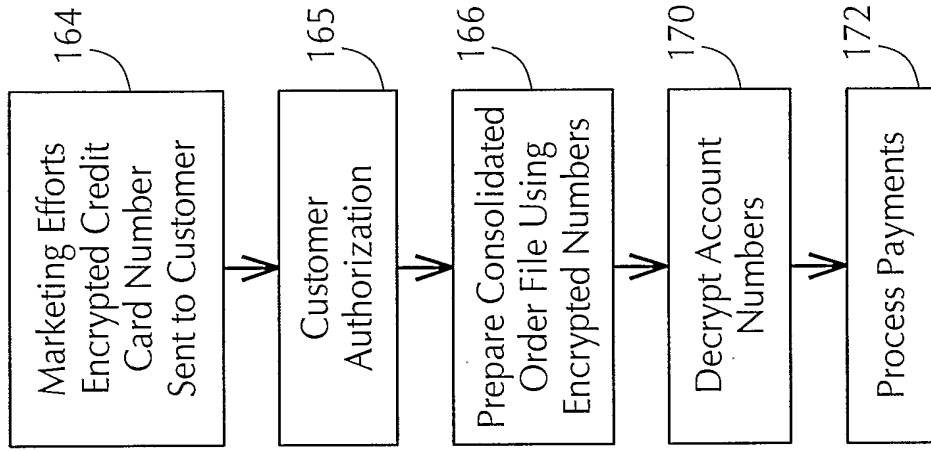


FIG. 7

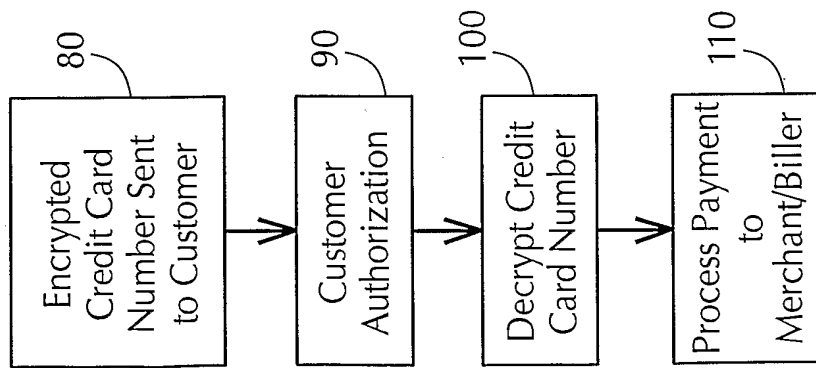


FIG. 4

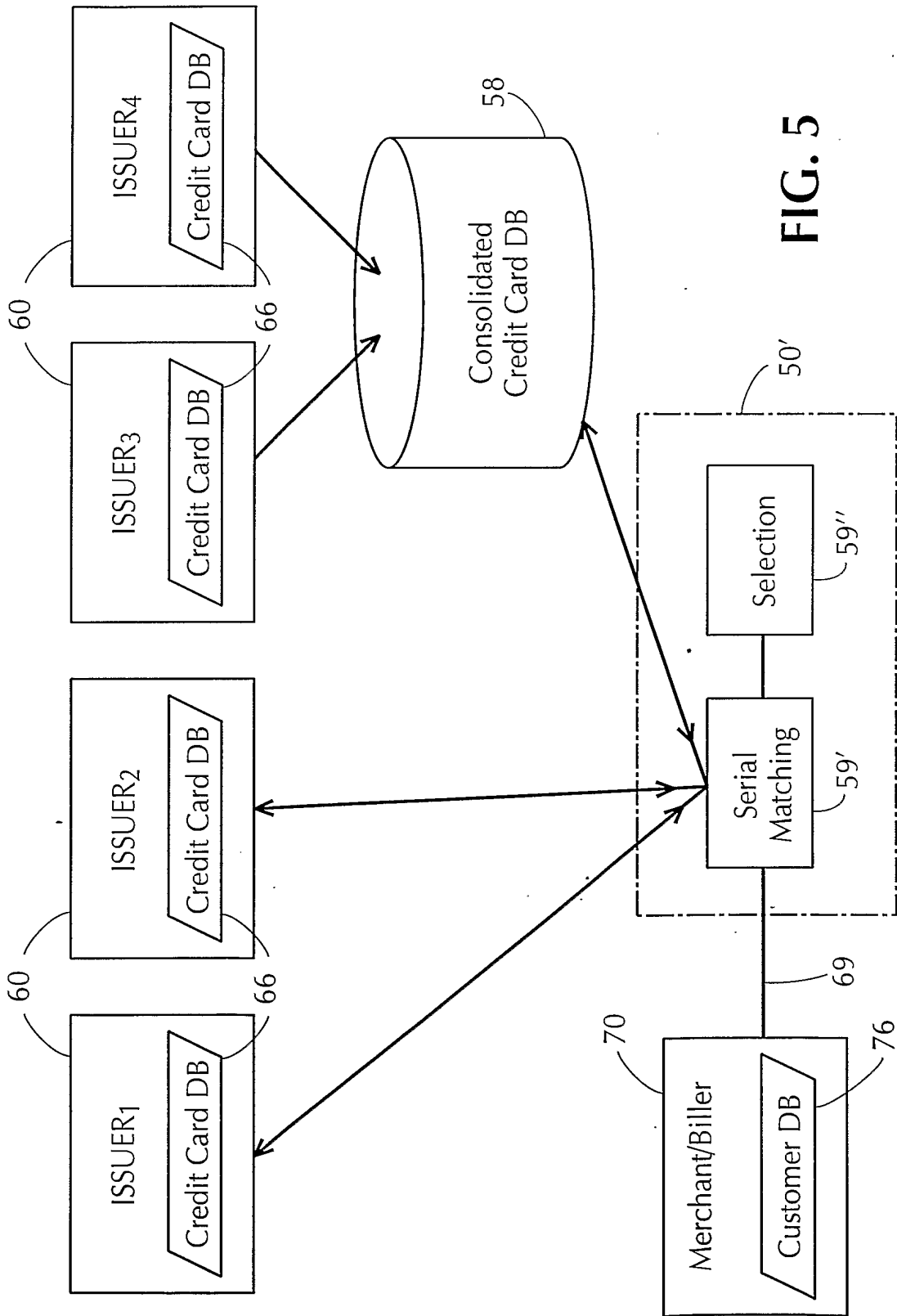


FIG. 5

FIG. 6

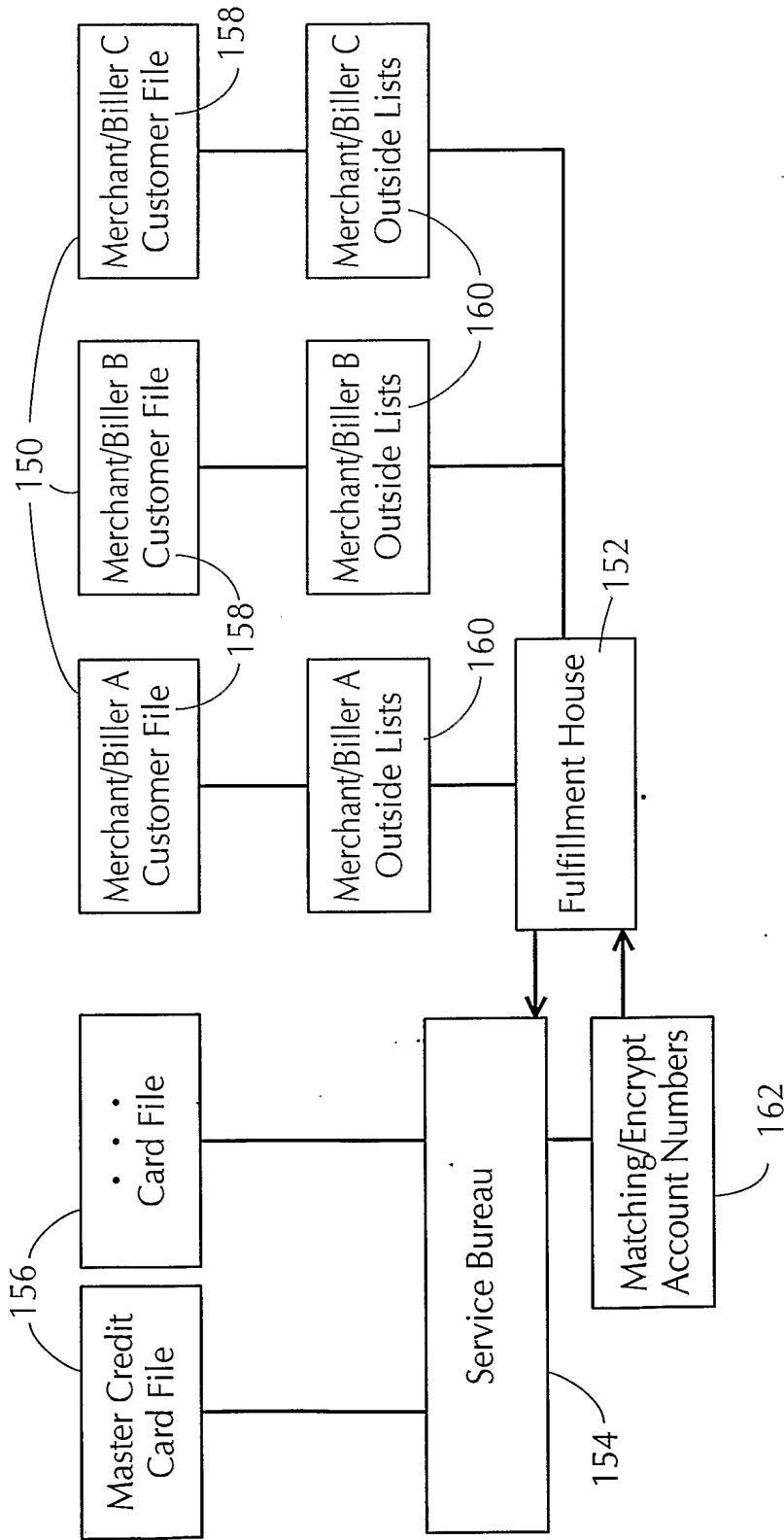
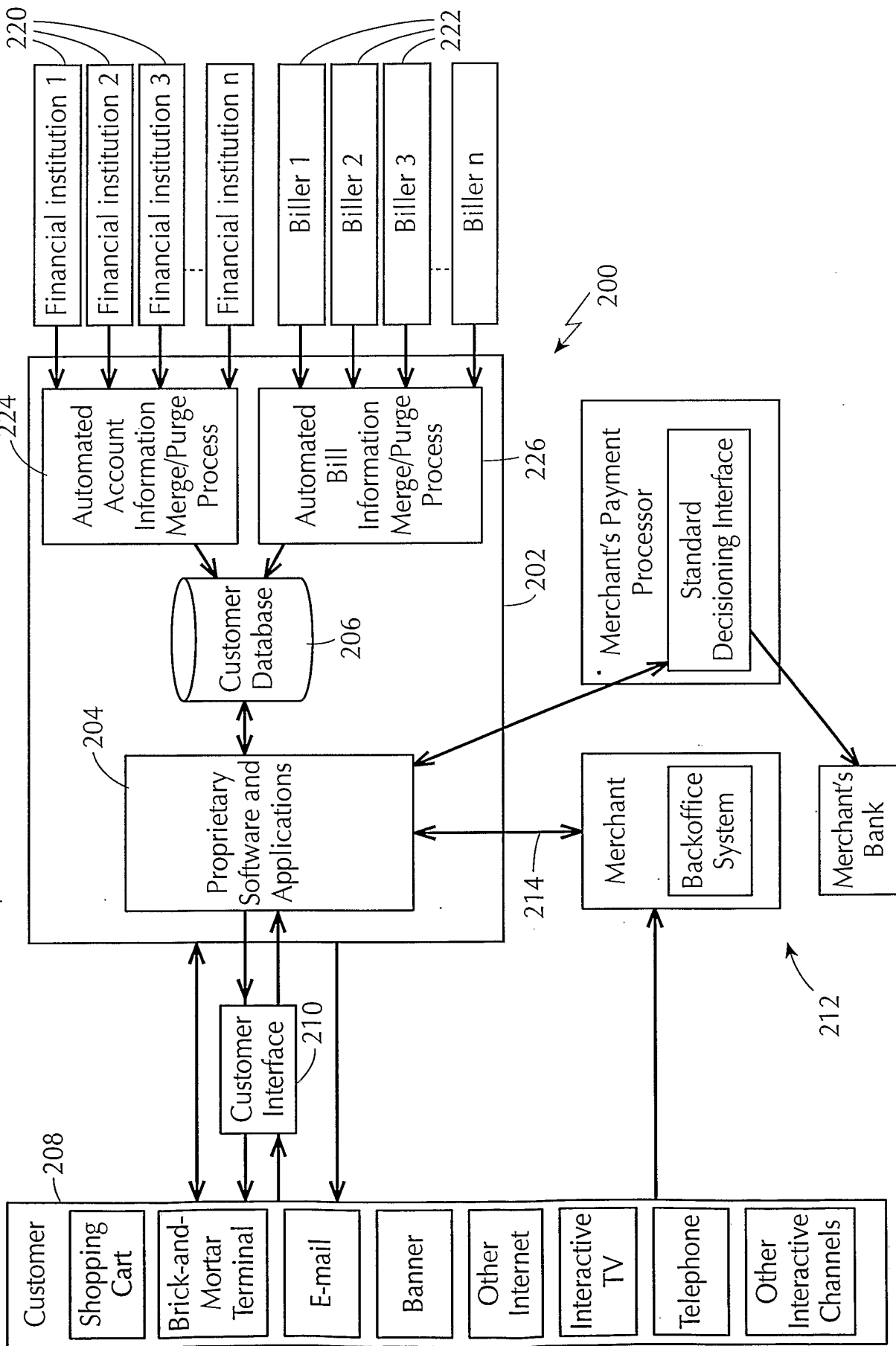


FIG. 8



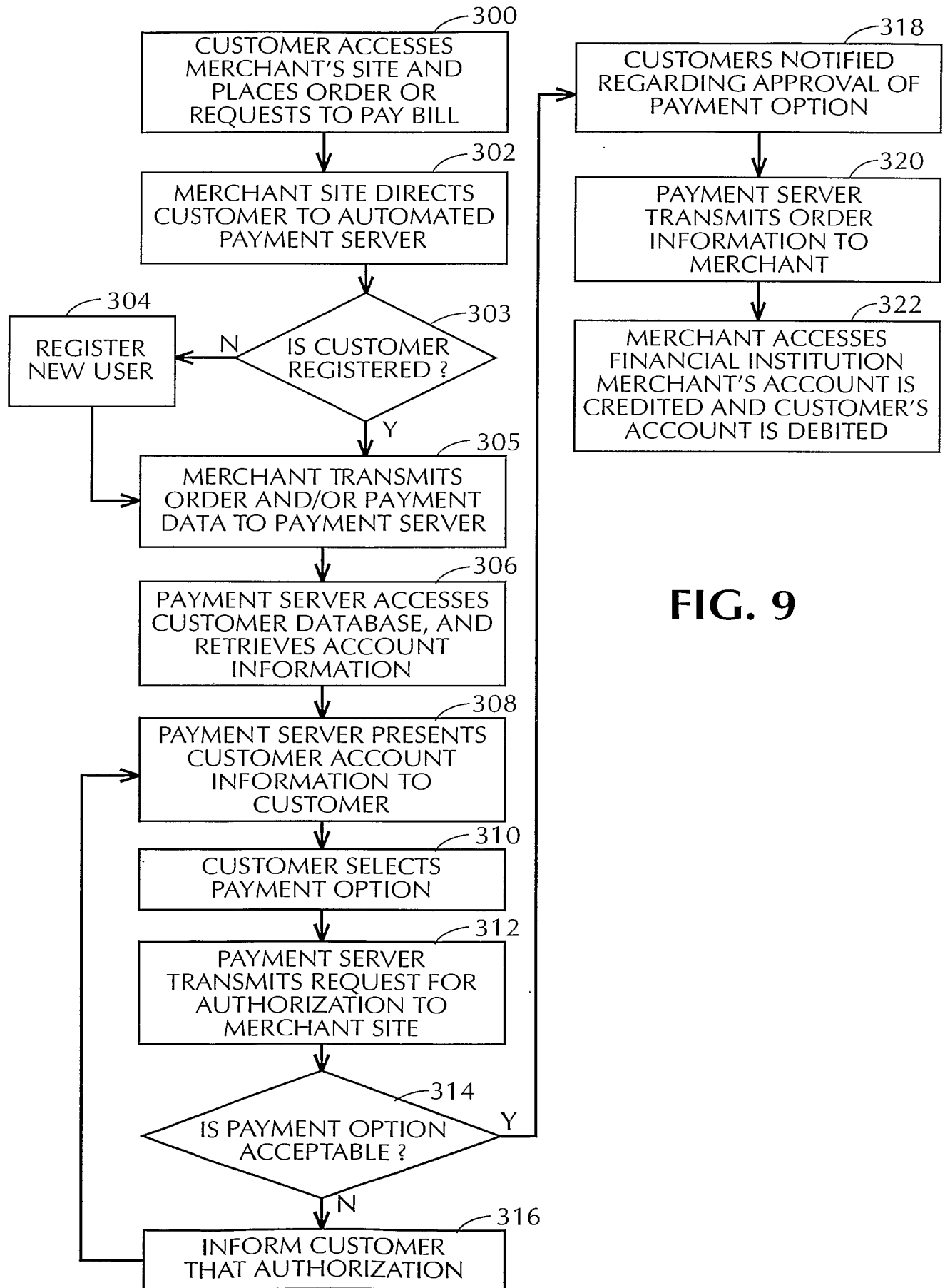


FIG. 9

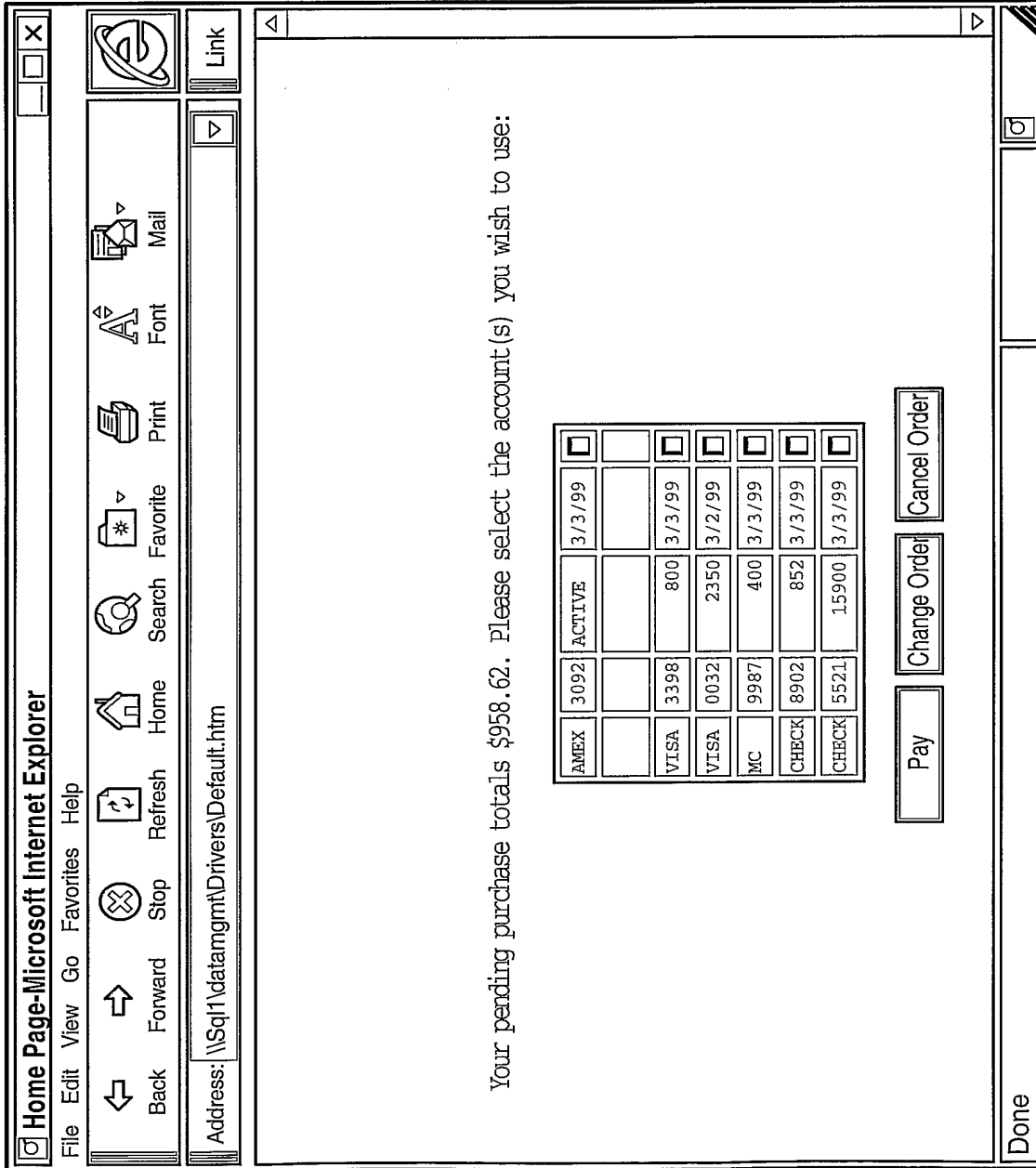


FIG. 10

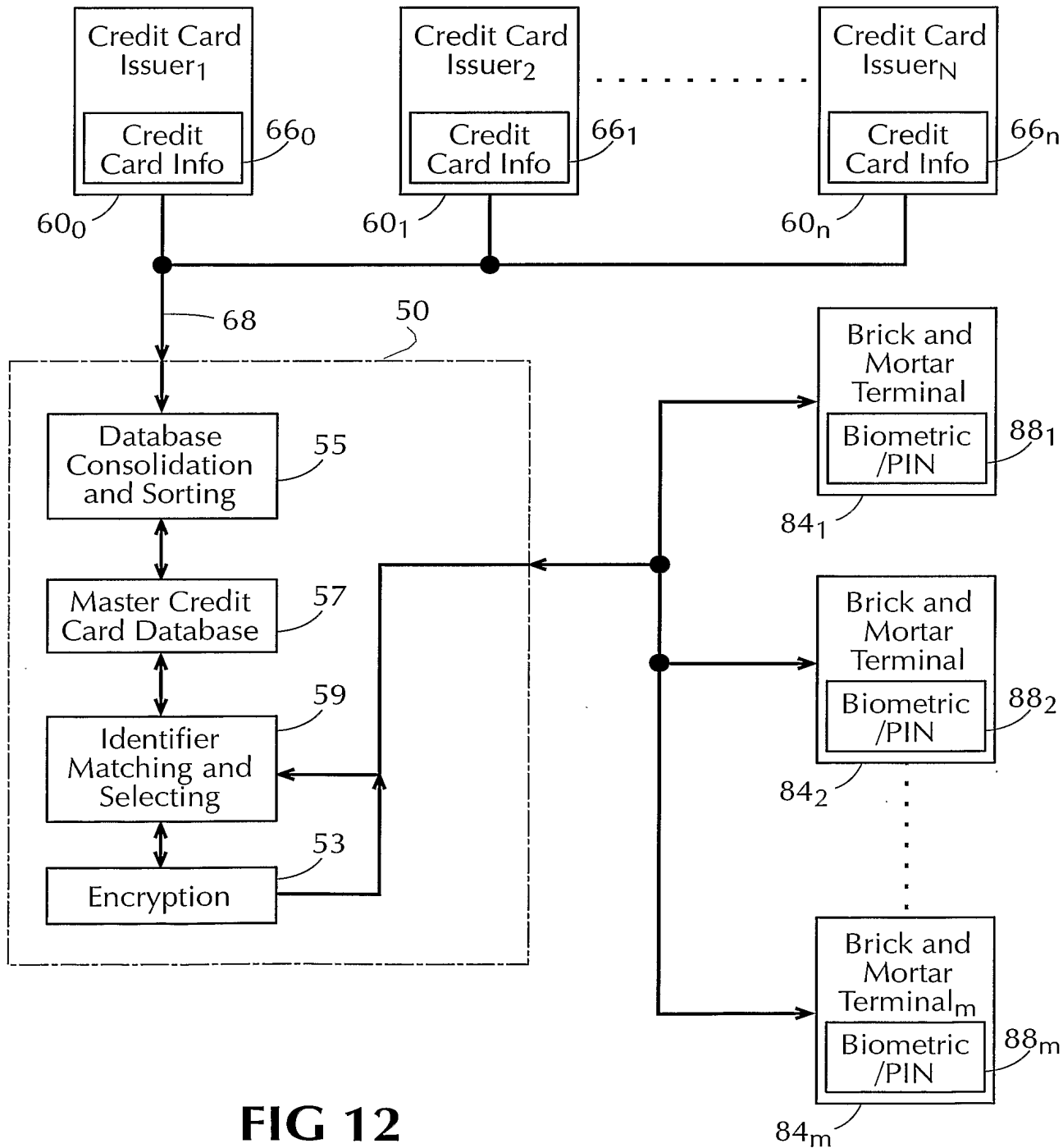


FIG 12

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US01/25888

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : G06F 17/60
US CL : 705/35

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 705/35, 39

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

DIALOG, DERWENT, WORLD WIDE WEB, EAST

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,P	US 2001/0001321 A1 (RESNICK et al.) 17 May 2001, see entire document.	1-96
X	US 5,987,132 A (ROWNEY) 16 November 1999, see entire document.	1-96
Y	US 5,963,926 A (KUMOMURA) 05 October 1999, see entire document.	1-96
Y	US 5,757,917 A (ROSE et al.) 26 May 1998, see entire document.	1-96

Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents:	"I"	Later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A" document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E" earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O" document referring to an oral disclosure, use, exhibition or other means		
"P" document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search: 24 JANUARY 2002
Date of mailing of the international search report: 13 FEB 2002

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks
Box PCT
Washington, D.C. 20231
Facsimile No. (703) 305-3230

Authorized officer: *Peggy Harrod*
KELLY SCAGGS
Telephone No. (703) 308-3900

Docket No.: W0537-700620

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Kenneth P. Weiss
Serial No: 11/768,729
Confirmation No: 3536
Filed: June 26, 2007
For: UNIVERSAL SECURE REGISTRY

Examiner: Dada, Beemnet W.
Art Unit: 2435

CERTIFICATE OF TRANSMISSION UNDER 37 C.F.R. §1.8(a)

The undersigned hereby certifies that this document is being electronically filed in accordance with § 1.6(a)(4), on the 24th day of May, 2010.

/Robert V. Donahoe/
Robert V. Donahoe, Reg. No. 46,667

Commissioner for Patents

PETITION FOR ONE MONTH EXTENSION OF TIME

Sir:

A one (1) month extension of time, to and including June 3, 2010, is requested for response to the Patent Office Communication of February 3, 2010.

The extension fee as set forth in 37 C.F.R. §1.17(a) is enclosed herewith.

Respectfully submitted,
Kenneth P. Weiss, Applicant

/Robert V. Donahoe/
Robert V. Donahoe, Reg. No. 46,667
LANDO & ANASTASI, LLP
Riverfront Office Park
One Main Street
Cambridge, Massachusetts 02142
Tel. (617) 395-7000

Electronic Patent Application Fee Transmittal

Application Number:	11768729
Filing Date:	26-Jun-2007
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Filer:	Robert Vincent Donahoe/Fareesha Ali
Attorney Docket Number:	W0537-7006

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 1 month with \$0 paid	2251	1	65	65

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Request for continued examination	2801	1	405	405
Total in USD (\$)				470

Electronic Acknowledgement Receipt

EFS ID:	7669583
Application Number:	11768729
International Application Number:	
Confirmation Number:	3536
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Correspondence Address:	John N. Anastasi c/o Lowrie, Lando & Anastasi, LLP Riverfront Office Park, One Main Street - Cambridge MA 02142 US 6173957000 -
Filer:	Robert Vincent Donahoe
Filer Authorized By:	
Attorney Docket Number:	W0537-7006
Receipt Date:	24-MAY-2010
Filing Date:	26-JUN-2007
Time Stamp:	16:33:40
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$470

RAM confirmation Number		3277			
Deposit Account		502762			
Authorized User					
File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	W0537-700620_RCE.pdf	697887	no	3
			d72c8a33d82b8a4900c951860fe320ab8c55cee3		
Warnings:					
Information:					
2	Information Disclosure Statement (IDS) Filed (SB/08)	W0537-700620_IDS_SB.pdf	612466	no	4
			1ad4566e361b0a4c3072d3c1f1edd13f00305911		
Warnings:					
Information:					
3	Foreign Reference	WO1996036934.pdf	7057142	no	206
			9bf3e4acee4a10cedc9020d455a7fe7b3b9869e7		
Warnings:					
Information:					
4	Foreign Reference	EP0986209.pdf	1603965	no	23
			8635936a39429c8c3c736ec5843ee3dab643ca87		
Warnings:					
Information:					
5	Foreign Reference	WO2002014985.pdf	2208001	no	52
			71afab2daefd744a30511d3ec2453372bc4cc960		
Warnings:					
Information:					
6	Extension of Time	W0537-700620_Extension_1.pdf	23898	no	1
			1362a0944e1d336a915d4e9db671a2f7b73d490f		
Warnings:					
Information:					
7	Fee Worksheet (PTO-875)	fee-info.pdf	32278	no	2
			072d389ea91534a5e9382e09f02c64bed064fe37		
Warnings:					
Information:					
Total Files Size (in bytes):			12235637		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 11/768,729	Filing Date 06/26/2007	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

APPLICATION AS FILED – PART I			OTHER THAN SMALL ENTITY				
	(Column 1)	(Column 2)	SMALL ENTITY <input checked="" type="checkbox"/>	OR			
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	OR	RATE (\$)	FEE (\$)
<input type="checkbox"/> BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>	N/A	N/A	N/A			N/A	
<input type="checkbox"/> SEARCH FEE <small>(37 CFR 1.16(k), (l), or (m))</small>	N/A	N/A	N/A			N/A	
<input type="checkbox"/> EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A	N/A			N/A	
TOTAL CLAIMS <small>(37 CFR 1.16(i))</small>	37 minus 20 =	*	X \$ =		OR	X \$ =	
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>	2 minus 3 =	*	X \$ =			X \$ =	
<input type="checkbox"/> APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.16(j))</small>							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY				
	(Column 1)	(Column 2)	(Column 3)		SMALL ENTITY	OR			
AMENDMENT	05/24/2010	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	* 37	Minus	** 34	=		OR	X \$ =	
	Independent <small>(37 CFR 1.16(h))</small>	* 2	Minus	*** 3	=		OR	X \$ =	
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>								
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>						OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

	(Column 1)	(Column 2)	(Column 3)		SMALL ENTITY	OR			
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	OR	RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	*	Minus	**	=		OR	X \$ =	
	Independent <small>(37 CFR 1.16(h))</small>	*	Minus	***	=		OR	X \$ =	
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>								
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>						OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
 ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
 *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".

Legal Instrument Examiner:
 /PEGGY YARBOROUGH/

The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
11/768,729 06/26/2007 Kenneth P. Weiss W0537-7006 3536

7590 12/22/2010
John N. Anastasi
c/o Lowrie, Lando & Anastasi, LLP
Riverfront Office Park, One Main Street
Cambridge, MA 02142

EXAMINER

DADA, BEEMNET W

ART UNIT PAPER NUMBER

2435

MAIL DATE DELIVERY MODE

12/22/2010

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 11/768,729	Applicant(s) WEISS, KENNETH P.	
	Examiner BEEBNET W. DADA	Art Unit 2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 24 May 2010.
- 2a) This action is **FINAL**.
- 2b) This action is non-final.
- 3) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) Claim(s) 1-5, 9-16, 18-21, 24-30, 32-39 and 41-45 is/are pending in the application.
 - 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) Claim(s) _____ is/are allowed.
- 6) Claim(s) 1-5, 9-16, 18-21, 24-30, 32-39 and 41-45 is/are rejected.
- 7) Claim(s) _____ is/are objected to.
- 8) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) The specification is objected to by the Examiner.
- 10) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
 - Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
 - Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
 - a) All b) Some * c) None of:
 - 1. Certified copies of the priority documents have been received.
 - 2. Certified copies of the priority documents have been received in Application No. _____.
 - 3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) Interview Summary (PTO-413)
Paper No(s)/Mail Date _____.
- 5) Notice of Informal Patent Application
- 6) Other: _____.

DETAILED ACTION

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 05/24/2010 has been entered. Claims 1-5, 9-16, 18-21, 24-30, 32, 34, 36 and 38 have been amended and new claims 41-45 have been added. Claims 1-5, 9-16, 18-21, 24-30, 32-39 and 41-45 are pending.

Response to Arguments

Applicant's arguments filed May 24, 2010 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-5, 9-16, 18-21, 24-30, 32-39 and 41-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gioradano et al. US 7,571,139 B1 (hereinafter Gioradano) in view Brainard et al. US 2006/0256961 A1 (hereinafter Brainard).

Art Unit: 2435

As per claims 1 and 16, Giorandano teaches a secure registry system for providing information to a service provider to enable the service provider to provide services to entities with secure data stored in the secure registry system, comprising:

a database including secure data for each entity, wherein each entity is associated with and a time-varying multicharacter_code for each entity having secure data in the secure registry system, respectively [column 18, lines 14-47] and

a processor configured to receive, from the service provider, the multicharacter code for the entity on whose behalf services are to be provided, configured to map the multicharacter code to secure data including information required to provide the services, the information including account identifying information where the account identifying information is unknown to the service provider, to provide the account identifying information to a third party to enable a transaction without providing the account identifying information to the service provider (i.e., note that the POS system does not get access to customers credit/debit account information, column 18, lines 5-47). Giorandano does not explicitly teach a time-varying code. In the same field of endeavor, Brainard teaches an authentication system including a time-varying multicharacter code to secure data and data access [paragraphs 0019 and 0020]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Brainard within the system of Gioradano in order to enhance the security of the system.

As per claims 2 and 18, Gioradano further teaches the system wherein the multicharacter code represents an identity of the entity [column 18, lines 14-47].

Art Unit: 2435

As per claims 3 and 19, Gioradano further teaches the system wherein the multicharacter code is provided to the system via a secure electronic transmission device [column 18, lines 14-47].

As per claim 4 and 20, Gioradano further teaches the system wherein the code is encrypted and transmitted to the system and wherein the system is configured to decrypt the code with a public key of the entity [column 18, lines 14-47].

As per claims 5 and 21, Gioradano further teaches the system wherein said service provider's service includes delivery, wherein the information is an address to which an item is to be delivered to the entity, wherein the system receives the code and wherein the system uses the code to obtain the appropriate address for delivery of the item by the third party [column 18, lines 14-47].

As per claim 9-15, 41-45, 24-27, 30, 32 and 41-45 Gioradano further teaches the system wherein the account identifying information includes credit card information regarding the entity and the processor is configured to provide the credit card information based upon the code of the entity to enable the transaction [column 18, lines 14-47].

As per claims 28-29 and 33-39, Gioradano further teaches the system wherein the database is further configured to associate biometric information with each entity having secure data in the secure registry respectively [column 18, lines 14-47].

Conclusion

Art Unit: 2435

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BEEMNET W. DADA whose telephone number is (571)272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Beemnet W Dada/
Primary Examiner, Art Unit 2435
December 20, 2010

Notice of References Cited	Application/Control No. 11/768,729	Applicant(s)/Patent Under Reexamination WEISS, KENNETH P.	
	Examiner BEEUNET W. DADA	Art Unit 2435	Page 1 of 1

U.S. PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A US-2006/0256961	11-2006	Brainard et al.	380/044
*	B US-7,571,139	08-2009	Giordano et al.	705/40
	C US-			
	D US-			
	E US-			
	F US-			
	G US-			
	H US-			
	I US-			
	J US-			
	K US-			
	L US-			
	M US-			

FOREIGN PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N				
	O				
	P				
	Q				
	R				
	S				
	T				

NON-PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)				
	U				
	V				
	W				
	X				

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes *1176872 9*	Application/Control No. 11768729	Applicant(s)/Patent Under Reexamination WEISS, KENNETH P.
	Examiner BEEMNET W DADA	Art Unit 2435

SEARCHED			
Class	Subclass	Date	Examiner
713	169, 182, 184	12/20/10	BD
707	9	12/20/10	BD

SEARCH NOTES		
Search Notes	Date	Examiner
East search	12/20/10	BD
IEEE, Google, Citeseer	12/20/10	BD
Inventor name search	12/20/10	BD

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

--	--

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11768729
	Filing Date	2007-06-26
	First Named Inventor	Kenneth P. Weiss
	Art Unit	2435
	Examiner Name	Dada, Beemnet W.
	Attorney Docket Number	W0537-700620

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1					

If you wish to add additional U.S. Patent citation information please click the Add button.

Add

U.S.PATENT APPLICATION PUBLICATIONS						Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20010044900		2001-11-22	Uchida	
	2	20030115490		2003-06-19	Russo et al.	
	3	20050187843		2005-08-25	Lapsley et al.	
	4	20050001711		2005-01-06	Doughty	
	5	20060016884		2006-01-26	Block et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button.

Add

FOREIGN PATENT DOCUMENTS						Remove
--------------------------	--	--	--	--	--	--------

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	11768729
Filing Date	2007-06-26
First Named Inventor	Kenneth P. Weiss
Art Unit	2435
Examiner Name	Dada, Beemnet W.
Attorney Docket Number	W0537-700620

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² i	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	1996036934	WO		1996-11-21	Smart Touch, L.L.C.		<input type="checkbox"/>
	2	0 986 209	EP		2000-03-15	Mitsubishi Denki Kabushiki Kaisha		<input type="checkbox"/>
	3	2002014985	WO		2002-02-21	Kern		<input type="checkbox"/>

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1		<input type="checkbox"/>

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Beemnet Dada/	Date Considered	12/20/2010
--------------------	----------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BD/

Docket No.: W0537-700620

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Kenneth P. Weiss
Serial No: 11/768,729
Confirmation No: 3536
Filed: June 26, 2007
For: UNIVERSAL SECURE REGISTRY

Examiner: Dada, Beemnet W.
Art Unit: 2435

CERTIFICATE OF TRANSMISSION UNDER 37 C.F.R. §1.8(a)

The undersigned hereby certifies that this document is being electronically filed in accordance with § 1.6(a)(4), on the 18th day of April, 2011.

/Robert V. Donahoe/
Robert V. Donahoe, Reg. No. 46,667

Commissioner for Patents

RESPONSE

Sir:

In response to the final Office Action mailed December 22, 2010, please enter the following response in the above-identified application.

Remarks begin on page 2 of this paper.

REMARKS

Claims 1-5, 9-16, 18-21, 24-30, 32-39 and 41-45 are currently pending for examination with claims 1 and 16 being independent claims. No amendments are included herein.

Rejections Under 35 U.S.C. §103(a)

The Office Action rejects claims 1-5, 9-16, 18-21, 24-30, 32-39 and 41-45 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 7,571,139 to Giordano et al. (hereinafter Giordano) in view of U.S. Publication No. 2006/0256961 to Brainard et al. (hereinafter Brainard). This rejection includes a rejection of each of the pending independent claims 1 and 16. Applicant respectfully asserts that the pending claims are patentable in view of the asserted combination at least because Giordano and Brainard either alone or in proper combination do not teach or suggest either “a processor ... *configured to map the time-varying multicharacter code to secure data including information required to provide the services*, the information including account identifying information where the account identifying information is unknown to the service provider,” as recited in claim 1, or a method including “*mapping the time-varying multicharacter code to information required to provide the services*, the information including account identifying information unknown to the service provider,” as recited in claim 16.

The Office Action states and Applicant agrees that Giordano “does not explicitly teach a time-varying code.” (Office Action at page 3.) The Office Action then asserts that Brainard teaches an “authentication system including a time-varying multicharacter code.” Id. Applicant notes that the Office Action does not assert that any reference teaches or suggests *mapping a time-varying multi-character code* to secure data including *information required to provide services* where the information includes “*account identifying information ... unknown to the service provider*,” as recited in claims 1 and 16. Accordingly, the Office Action fails to establish a proper prima facie case of obviousness for at least this reason.

In addition, Applicant respectfully submits that the cited references do not teach or suggest the preceding. For example, paragraph 19 of Brainard merely describes generating an authentication code in response to the verifier seed and a time dependent value and then authenticating a user by verifying the authentication code. Applicant respectfully asserts that the

preceding, whether alone or in proper combination with Giordano, does not teach or suggest *mapping a time-varying multi-character code* to secure data including *information required to provide services* where the information includes “*account identifying information ... unknown to the service provider,*” as recited in claims 1 and 16.

Accordingly, each of claims 1 and 16 are patentable for at least the reasons described above. Each of claims 2-5, 9-15, 18-21, 24-30, 32-39 and 41-45 depend from one of the allowable independent claims and is allowable for at least for the same reasons as the independent claim from which it depends. For at least these reasons, Applicant requests reconsideration and withdrawal of the rejection of claims 1-5, 9-16, 18-21, 24-30, 32-39 and 41-45.

Applicant also notes that the Office Action states that “as per claims 28-29 and 33-39, Giordano further teaches the system wherein the database is further configured to associate biometric information with each entity having secure data in the secure registry respectively [column 18, lines 14-47].” Applicant respectfully disagrees with the preceding and asserts that claims 28-29 and 33-39 are patentable for reasons in addition to their dependency from an allowable base claim.

Specifically, Giordano teaches activation of a *customer transceiver* 50 based on a customer provided biometric. (Col. 13, lines 23-26; see also, claims 3-6.) In Giordano, the biometric is unavailable to other elements of the system 30. *Id.* Accordingly, Giordano does not teach or suggest any of: a “database is further configured to associate biometric information with each entity having secure data in the secure registry, respectively,” as recited in claim 33; a “processor is further configured to map the time-varying multicharacter code to biometric information associated with the entity on whose behalf the services are to be provided and to provide the biometric information to the service provider,” as recited in claim 34; and “wherein the biometric information includes an image of the entity on whose behalf the services are to be provided,” as recited in claim 35.

General Comments on Dependent Claims

Since each of the rejected dependent claims depends from a base claim that is believed to be in condition for allowance, Applicant believes that it is unnecessary at this time to argue the

allowability of each of the dependent claims individually. However, Applicant does not necessarily concur with the interpretation of the rejected dependent claims as set forth in the Office Action, nor does Applicant concur that the basis for the rejection of any of the dependent claims is proper. Therefore, Applicant reserves the right to specifically address the patentability of the dependent claims in the future, if deemed necessary.

CONCLUSION

In view of the foregoing amendments and remarks, reconsideration is respectfully requested. This application should now be in condition for allowance; a notice to this effect is respectfully requested. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicant's attorney at the telephone number listed below.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee that is not covered by an accompanying payment, please charge any deficiency to Deposit Account No. 50/2762, Ref. No. W0537-700620.

Respectfully submitted,
Kenneth P. Weiss, Applicant

By: /Robert V. Donahoe/
Robert V. Donahoe, Reg. No. 46,667
LANDO & ANASTASI, LLP
One Main Street
Cambridge, Massachusetts 02142
United States of America
Telephone: 617-395-7000
Facsimile: 617-395-7070

Docket No.: W0537-700620

Date: April 18, 2011

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Kenneth P. Weiss
Serial No: 11/768,729
Confirmation No: 3536
Filed: June 26, 2007
For: UNIVERSAL SECURE REGISTRY

Examiner: Dada, Beemnet W.
Art Unit: 2435

CERTIFICATE OF TRANSMISSION UNDER 37 C.F.R. §1.8(a)

The undersigned hereby certifies that this document is being electronically filed in accordance with § 1.6(a)(4), on the 18th day of April, 2011.

/Robert V. Donahoe/
Robert V. Donahoe, Reg. No. 46,667

Commissioner for Patents

**INFORMATION DISCLOSURE STATEMENT FILED PURSUANT TO THE DUTY OF
DISCLOSURE UNDER 37 CFR §§1.56, 1.97 AND 1.98**

Sir:

Pursuant to the duty of disclosure under 37 C.F.R. §§1.56, 1.97 and 1.98, the Applicant requests consideration of this Information Disclosure Statement.

PART I: Information Cited

The Applicant hereby makes of record in the above-identified application the information listed on the concurrently filed form PTO/SB/08a.

The order of presentation of the references should not be construed as an indication of the importance of the references.

The Applicant hereby makes the following additional information of record in the above-identified application.

The applicant would like to bring to the Examiner's attention the following co-pending applications that may contain subject matter related to this application:

Serial No.	Filing Date	Inventor	Patent No.
09/810703	16-Mar-2001	Kenneth P. Weiss	7,237,117
11/677490	21-Feb-2007	Kenneth P. Weiss	Pending
11/760732	08-Jun-2007	Kenneth P. Weiss	7,809,651
11/760729	08-Jun-2007	Kenneth P. Weiss	7,805,372
12/393586	26-Feb-2009	Kenneth P. Weiss	Pending

PART II: Remarks

Documents cited anywhere in the Information Disclosure Statement, other than U.S. Patents and U.S. Patent Application Publications listed on a Form PTO/SB/08a, are enclosed unless otherwise indicated. It is respectfully requested that:

1. The Examiner consider completely the cited information, along with any other information, in reaching a determination concerning the patentability of the present claims;
2. Any concurrently filed form PTO/SB/08a be signed by the Examiner to evidence that the cited information has been fully considered by the Patent and Trademark Office during the examination of this application;
3. The citations for the information be printed on any patent which issues from this application.

By submitting this Information Disclosure Statement, the Applicant makes no representation that a search has been performed, of the extent of any search performed, or that more relevant information does not exist.

By submitting this Information Disclosure Statement, the Applicant makes no representation that the information cited in the Statement is, or is considered to be, material to patentability as defined in 37 C.F.R. §1.56(b).

By submitting this Information Disclosure Statement, the Applicant makes no representation that the information cited in the Statement is, or is considered to be, in fact, prior art as defined by 35 U.S.C. §102.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11768729
	Filing Date	2007-06-27
	First Named Inventor	Kenneth P. Weiss
	Art Unit	2435
	Examiner Name	Dada, Beemnet W.
	Attorney Docket Number	W0537-700620

U.S.PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1	6309342		2001-10-30	Blazey et al.		
	2	6819219		2004-11-16	Bolle et al.		

If you wish to add additional U.S. Patent citation information please click the Add button.

Add

U.S.PATENT APPLICATION PUBLICATIONS							Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1						

If you wish to add additional U.S. Published Application citation information please click the Add button.

Add

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² j	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	1 081 632	EP		2001-07-03	Keyware Technologies		<input type="checkbox"/>
	2	2 382 006	GB		2003-05-14	IBM		<input type="checkbox"/>

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11768729
	Filing Date	2007-06-27
	First Named Inventor	Kenneth P. Weiss
	Art Unit	2435
	Examiner Name	Dada, Beemnet W.
	Attorney Docket Number	W0537-700620

3	1992007436	WO		1992-04-30	Security Dynamics Limited, Inc.	<input type="checkbox"/>
---	------------	----	--	------------	---------------------------------	--------------------------

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	"FIPS PUB 46-3." 25 October 1999. National Institute of Science and Technology (NIST).	<input type="checkbox"/>
	2	"PGP: An Introduction to Cryptography." 2000.	<input type="checkbox"/>
	3	International Search Report from PCT/US2007/070701 mailed March 11, 2008.	<input type="checkbox"/>
	4	International Search Report from PCT/US2007/004646 mailed November 27, 2007.	<input type="checkbox"/>
	5	International Search Report from PCT/US2009/035282 mailed July 10, 2009.	<input type="checkbox"/>
	6	Pabrai, U. "Biometrics for PC-User Authentication: A Primer" 1 February 2001. Access Controls & Security Systems. All pages. < http://www.securitysolutions.com/mag/security_biometrics_puser_authentication/index.html >	<input type="checkbox"/>

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	11768729
Filing Date	2007-06-27
First Named Inventor	Kenneth P. Weiss
Art Unit	2435
Examiner Name	Dada, Beemnet W.
Attorney Docket Number	W0537-700620

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	11768729
Filing Date	2007-06-27
First Named Inventor	Kenneth P. Weiss
Art Unit	2435
Examiner Name	Dada, Beemnet W.
Attorney Docket Number	W0537-700620

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Robert V. Donahoe/	Date (YYYY-MM-DD)	2011-04-18
Name/Print	Robert V. Donahoe	Registration Number	46667

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.



Europäisches Patentamt
European Patent Office
Office européen des brevets



(11) **EP 1 081 632 A1**

(12) **EUROPEAN PATENT APPLICATION**

(43) Date of publication:
07.03.2001 Bulletin 2001/10

(51) Int Cl.7: **G06K 9/68**

(21) Application number: **99870178.3**

(22) Date of filing: **01.09.1999**

(84) Designated Contracting States:
**AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE**
Designated Extension States:
AL LT LV MK RO SI

(72) Inventor: **KEYWARE TECHNOLOGIES,
c/o Declercq Francis
B-1930 Zaventem (BE)**

(71) Applicant: **Keyware Technologies
8900 Ieper (BE)**

(74) Representative: **Quintelier, Claude et al
Gevers & Vander Haeghen,
Patent Attorneys,
Rue de Livourne 7
1060 Brussels (BE)**

(54) **Biometric authentication device**

(57) A biometric authentication device provided for managing access to at least one entity, said device being connectable to a database storing biometric templates, said device comprising a set of bio-engines and a data capture unit provided to collect life biometric data, each of said bio-engines being provided for performing a dedicated biometric authentication operation with said biometric templates and said life biometric data and for generating a score as a result of said authentication operation, said device comprises a decision unit operating according to a master-slave relationship, wherein said

decision unit being the master, said decision unit being provided for receiving each of said scores and for assigning a respective weight factor to each of said scores and forming a set of weighted scores therewith, said decision unit being further provided for combining said weighted scores and generating a verified score therewith, said decision unit being also provided for comparing said verified score with a threshold value and for generating an access enable signal as a result of a positive comparison and an access refusal signal as a result of a negative comparison.

EP 1 081 632 A1

Description

[0001] The present invention relates to a biometric authentication device provided for managing access to at least one entity, said device being operatively connectable to a database provided for storing biometric templates, said device comprising a set of bio-engines each having an input for receiving said biometric templates and life biometric data originating from a data capture unit provided to collect life data, each of said bio-engines being provided for performing a dedicated biometric authentication operation with said biometric templates and said life biometric data and for generating a score as a result of said authentication operation.

[0002] Biometric authentication devices are known and their use is for example described in the article "Person authentication by fusing face and speech information" written by B. Duc, G. Maître, S. Fischer and J. Bigün and presented on the First International Conference AVBPA in Crans-Montana in March 1997 (p. 311-318). Biometrics is a science of measuring unique physical or behavioural characteristics such as the pattern of the voice of a person, or the micro-visual pattern of his retina, the tiny swirls etched in the skin of his fingertip, this facial appearance etc. Biometric authentication is used to manage access to an entity such as for example an office or a room, a bank account, a computer or a network, etc. The biometric data of one or more persons is stored in a database to which the bio-engines performing the biometric authentication have access. Data capture units such as for example a camera, a fingerprint scanner or a microphone collect the life biometric data from the person who want to get access to the entity protected by the biometric authentication device. The bio-engines perform than authentications and issue a score. If the score is above the predetermined threshold the person will get access to the entity. If the score is below the threshold access will be refused. The bio-engines are provided for a dedicated biometric authentication, i.e. there is a bio-engine for voice authentication, one for the fingerprint, another for the facial appearance etc. Each bio-engine generates its own score independent of the other engines.

[0003] Operating with a single bio-engine has a major drawback because the life biometric data of the person such as collected by the data capture unit can change. So for example a person having a cold will have his voice sound differently such that the bio-engine performing the voice authentication will issue a lower score which could lead to an access refusal. This could be solved by lowering the threshold. However lowering the threshold leads to an increase of false acceptance which for certain secure applications is unacceptable. Therefor attempts have been made to combine the outputs of several bio-engines such as described in the referred article.

[0004] A drawback of the known devices where the output of several biometric engines are combined is that

they do not enable a true combination of the scores as each bio-engine continues to operate on its own by generating its own decision based on its internal score.

[0005] It is an object of the invention to realise a biometric authentication device enabling a true combination of the scores of the different bio-engines.

[0006] A biometric authentication device according to the present invention is therefor characterized in that said device comprises a decision unit connected to said bio-engines and operating according to a master-slave relationship, wherein said decision unit being the master, said decision unit being provided for receiving each of said scores and for assigning a respective weight factor to each of said scores and forming a set of weighted scores therewith, said decision unit being further provided for combining said weighted scores and generating a verified score therewith, said decision unit being also provided for comparing said verified score with a threshold value and for generating an access enable signal as a result of a positive comparison and an access refusal signal as a result of a negative comparison. The master-slave governing the relationship between the decision unit and the bio-engines enables such a true combination as the bio-engines scores are weighted by the decision unit. If one score is for example below the threshold whereas the others are above their respective thresholds, the decision unit can reduce the impact of such a bio-engine by assigning a low weight factor. As the decision unit has the scores of the different bio-engines a relative weighing of the different scores becomes possible. The decision to enable or not access to the entity is thus no longer based on a combination of the individual outputs of the different bio-engines, but on a combination of the scores realised by the decision unit.

[0007] A first preferred embodiment of a biometric authentication device according to the invention is characterized in that the decision unit is connected with a first bio-decision engine which is provided for executing a serial combinatorial operation with the scores generated by at least one of said bio-engines, said first bio-decision engine being provided to operate as a slave from said decision unit. This enables to have each individual bio-engine performing several authentication operations and to serially combine the scores issued by a same bio-engine.

[0008] A second preferred embodiment of a biometric authentication device according to the invention is characterized in that the decision unit is connected with a second bio-decision engine, which is provided for executing a parallel combinatorial operation with the scores generated by at least one of said bio-engines, said second bio-decision engine being provided to operate as a slave from said decision unit. This enables to have each individual bio-engine performing several authentication operations and to combine in parallel the scores issued by a same bio-engine.

[0009] A third preferred embodiment of a biometric

authentication device according to the invention is characterized in that said decision unit is provided for generating a control signal when said verified score is below said threshold, said decision unit being further provided for determining a set of further weight factors under control of said control signal and assigning them to said scores and generating a further verified score therewith. This enables to reconsider the authentication operation if one of the scores was insufficient for example due to particular circumstances such a user having a bad voice quality due to a cold.

[0010] A fourth preferred embodiment of a biometric authentication device according to the invention is characterized in that said further weight factors and said weight factors each time satisfy a predetermined relationship. The weight factors are thus normalized which facilitates the calculation and keeps the verified score reliable.

[0011] Preferably said decision unit comprises a core server which is provided for generating said verified score and executing said comparison. This facilitates the architectural structure of the device.

[0012] Preferably characterized in that said decision unit comprises a module manager which is provided for managing data traffic between said bio-engines and said core server. An improved architecture for the data traffic is thus obtained.

[0013] Preferably said data capture unit is connected to an interface to which a feature module is connected, said feature module being provided for input of client dedicated features. The end user can in such a manner supply his own particular features to the device, such as for example those relating to a particular group of users or relating to particularities of individual users.

[0014] A fifth preferred embodiment of a biometric authentication device according to the invention is characterized in that said biometric templates are stored in a memory formed by either a smartcard, a harddisk, a EEPROM or a flash memory. In particular when a smartcard is used, the biometric templates of the owner are stored thereon and there is no need to let them travel over a publicly accessible network.

[0015] A sixth preferred embodiment of a biometric authentication device according to the invention is characterized in that said decision unit is connected to a self learning module which is provided for substituting into said database a biometric template by a life biometric data under control of a second control signal generated by said decision unit upon detection of a score issued by a bio-engine which is higher than a further predetermined threshold value. This enables to up-date the biometric templates and thus to improve the reliability of the access monitoring.

[0016] A seventh preferred embodiment of a biometric authentication device according to the invention is characterized in that said decision unit is connected to an environmental module which is provided for generating a trigger signal, said decision unit being provided

to modify the weight factors under control of said trigger signal. This enables to take into account environmental conditions such as background noise or high or pour light intensity.

[0017] The invention will now be described in more details by means of the drawings showing a preferred embodiment of a device according to the invention. In the drawings :

Figure 1 illustrates the relation between a False Accept Rate and a False Reject Rate;

Figure 2 illustrates serial operating bio-engines;

Figure 3 illustrates parallel operating bio-engines;

Figure 4 illustrates a combination of parallel and serial operating bio-engines;

Figure 5 illustrates a set-up of different bio-engines according to the state of the art;

Figure 6 illustrates the principle of a threshold in a bio-engine;

Figure 7 illustrates schematically a set-up of a biometric authentication device according to the present invention;

Figure 8 illustrates the architecture of a biometric authentication device according to the present invention; and

Figure 9 illustrates schematically the operation of a biometric authentication device according to the present invention.

[0018] In the drawings a same reference sign has been assigned to a same or analogous element.

[0019] In biometrics a distinction is made between a "client", who should be recognised as somebody having access to the protected entity and an "impostor" who is someone pretending to be someone else and who should not have access. The protected entity can be a room, an office, a bank account, a computer system, a network etc.

[0020] The False Acceptance Rate (FAR) gives the percentage of falsely accepted impostors

$$FAR = \frac{\text{total number of falsely accepted impostors}}{\text{total number of impostors tested}}$$

[0021] The False Rejection Rate (FRR) gives the percentage of falsely rejected clients.

$$FRR = \frac{\text{total number of falsely rejected clients}}{\text{total number of clients tested}}$$

[0022] The Equal Error Rate (EER) is the percentage corresponding to the threshold level for which the FAR and FRR are equal. Figure 1 illustrates the relation between FAR and FRR. FAR and FRR are inversely proportional as illustrated. The technology tries to lower the EER which is the cross point between the FAR - FRR curve and the curve $y = x$. To lower the EER it is necessary to lower the values of FAR and FRR This can be

obtained by increasing the number of biometric authentications.

[0023] Authentication signifies the general process of verifying the identity claimed by the user. Authentication thus covers as well a authentication process, which is a one to one process, as an identification process, which is a one to many process. Identification answers the question "Who is trying to get in ?", whereas authentication answers the question "Is that really Mr. Jones trying to get in ?" Biometric authentication is used as a general term for a process of checking ones identity by biometric technology.

[0024] A first possibility for increasing the number of biometric authentications is to serially combine the biometric authentication operations such as illustrated in figure 2. Suppose that two biometric authentication operations are performed, one by bio-engine A which performs a voice authentication and one by bio-engine B which performs face authentication. The serial combination starts with the first bio-engine generating a score Sva.

[0025] Due to the serial arrangement the second bio-engine B can only generate a score Svb if the first bio-engine has generated a positive score, i.e. if the first authentication was successful. The FAR_S of the whole system is determined by :

$$FAR_S = FAR_A \times FAR_B$$

The FRR_S of the system is determined by

$$FRR_S = FFR_A + (1 - FRR_A) \times FRR_B$$

By way of example suppose now

$$EER_A = 5 \% \text{ and } EER_B = 2 \%$$

Suppose also that both bio-engines will operate at a threshold where the EER is obtained. The threshold being the value of the score such as generated by the bio-engine at which a positive result i.e. access enabled, is generated. So FAR_A = FRR_A = 5 % and FAR_B = FRR_B = 2%. The serial system will then have the following values :

$$FAR_S = 0.05 \times 0.02 = 0.001 \text{ or } 0.1 \%$$

$$FRR_S = 0.05 + (1 - 0.05) \times 0.02 = 0.069 \text{ or } 6.9 \%$$

Thus the serial combination offers a better FAR_S than each individual system but the FRR_S has become worse. So with a serial combination it is harder to get falsely accepted because one has to pass two or more

authentications, but the probability of being falsely refused has substantially increased.

[0026] A second possibility for increasing the number of biometric authentications is to combine the biometric operations in parallel as illustrated in figure 3. In such a configuration the user has two attempts which are performed independently from each other. The acceptance of a user by one of the engines will not reroute the authentication procedure to the other. If a person is not accepted by one of the engines he could still be accepted by the other. Combining both systems will provide an overall performance with :

$$FAR_S = FAR_A + FAR_B - FAR_A \times FAR_B$$

$$FRR_S = FRR_A \times FRR_B$$

Going back to the example with FAR_A = FRR_A = 5 % and FAR_B = FRR_B = 2 % the following results are obtained :

$$FAR_S = 0.05 + 0.02 - 0.05 \times 0.02 =$$

$$0.07 - 0.001 = 0.069 \text{ or } 6.9 \%$$

$$FRR_S = 0.05 \times 0.02 = 0.001 \text{ or } 0.1 \%$$

Thus a parallel combinatorial system has a better FRR_S than each of the individual system, but the FAR_S has substantially increased.

[0027] A third possibility for increasing the number of biometric authentications is to form a combination of both parallel and serial combinations such as for example illustrated in figure 4. Each of the bio-engines performs in parallel several authentication processes and the output of the first layer of bio-engines (1) (for example the voice authentication) is serially combined to the second layer of bio-engines (2) (for example a fingerprint authentication). With such a set-up a user has three attempts with the first layer and if he is successful in one of those attempts he has again three attempts with the second layer. The overall performance of this system is now :

$$FAR_{S1} = FAR_{1a} + (1 - FAR_{1a}) \times FAR_{1b} \\ + (1 - FAR_{1a}) \times (1 - FAR_{1b}) \times FAR_{1c}$$

$$FRR_{S1} = FRR_{1a} \times FRR_{1b} \times FRR_{1c}$$

$$FAR_{S2} = FAR_{2a} + (1 - FAR_{2a}) \times FAR_{2b}$$

$$+ (1 - FAR_{2a}) \times (1 - FAR_{2b}) \times FAR_{2c}$$

$$FRR_{S2} = FRR_{2a} \times FRR_{2b} \times FRR_{2c}$$

$$FAR_{SS} = FAR_{S1} \times FAR_{S2}$$

$$FAR_{SS} = FRR_{S1} + (1 - FRR_{S1}) \times FRR_{S2}$$

Turning back to the example with $FAR_{1a,1b,1c} = FRR_{1a,1b,1c} = 5\%$

$$FAR_{2a,2b,2c} = FRR_{2a,2b,2c} = 2\%$$

the following results are obtained.

$$FAR_{SS} = 0.083 \text{ or } 8.3\%$$

$$FRR_{SS} = 0.0013 \text{ or } 0.13\%$$

This set-up thus provide an overall improvement since both the FAR and FRR have better values than the individual systems.

[0028] The theory set out here before shows thus by using several layers into an authentication scheme in a same session enables the combination of several biometric results. Figure 5 shows schematically an embodiment according to the state of the art of combining several bio-engines. The illustrated device comprises face authentication member 1, a fingerprint authentication member 2 and a voice authentication member 3 which are all connected to a Local Area Network 4 (LAN). Of course other members could be connected to the LAN but only three are shown for the sake of clarity. A firewall 5 protects the LAN from the outside publically accessible network 7 to which a netserver 6 is connected. The entity 8 to which access has to be managed is for example formed by an entrance door. Each of the members 1, 2 and 3 operate individually from each other and have there own server and their own database in which biometric templates are stored. Biometric templates being each time formed by a set of data comprising the biometric data belonging to one or more clients of which the access to the entity has to be controlled and who have access to the entity. So for example the biometric template of the face of Arthur Jones who has access to the building is formed by a set of data identifying the face of Arthur Jones.

[0029] In the device of figure 5 each of the members will perform there own authentication process by using their own database and own bio-engines and each bio-engine will issue a score which will be compared with

the threshold set in that bio-engine upon initializing that bio-engine. If the score of the bio-engine is higher than the threshold an acceptance signal will be issued and supplied to the LAN, if not a refusal signal is issued and supplied to the LAN. The score such as issued by the bio-engine is not available on the LAN.

[0030] As already mentioned each bio-engine provides a score which is thresholded to come to a decision being accept, reject or fuzzy. Each bio-engine has a performance curve that characterizes the technology involved and which is expressed by the EER.

[0031] Figure 6 shows a first curve (a) for the bonafide score and a second curve (b) for the impostor score. The vertical line (c) illustrates the set threshold value. If the score is higher than the threshold the user is accepted, if not he is rejected. In biometrics there is a typical trade-off between accepting users and rejecting them. Increasing the threshold will lower the false accept but will raise the false reject rate. Since biometrics, by their nature, are not deterministic the score obtained by the bio-engines may show variance over time. Typically a user either a bonafide or an impostor, will usually have a Gaussian distribution around his mean score.

[0032] Combining different biometrics, each with their specific FAR, FRR and EER enables to get a better performance. The biometric authentication device according to the present invention combines the outcome of different bio-engines at their result or score level and not at the level of the signals as it is the case for the device shown in figure 5. An example of a biometric authentication device according to the present invention is schematically illustrated in figure 7. The device comprises a LAN 10 to which a layered biometric platform 11 is connected. A firewall 16 is connected between the LAN 10 and the outside network 17 to which a web server 19 could also be connected. Different client modules 12 (a, b, c) can be connected to the platform 11. So for example module 12a is dedicated to particular client features for the LAN security, whereas module 12b respectively 12c is dedicated to particular client features for the web security and physical access to an entity such as a door 13. The different bio-engines performing the biometric authentication operation are now embedded in the platform. The centralization of all bio-engines 11a, 11b and 11c into one platform enables to centralize the storage of the bio-data and templates and to have a common logging and archiving environment. The platform has a common server operating with a common database which is either permanently embedded in the platform and for example formed by a hard disc or another memory, or is formed by a stand alone memory such as for example a smartcard which is connectable to the platform. The server is formed either by a relatively powerful computer, as biometric needs an intensive cpu work, or is formed by different processors provided to operate together.

[0033] Figure 8 illustrates an embodiment of the architecture of the platform and the client module of the

biometric authentication device according to the present invention. The client module 12 comprises one or more data capture units 20, depending on the biometric authentication to be performed. So for example if authentication is to be performed on the face, the fingerprint and the voice, the data capture unit will comprise a camera, a fingerprint scanner and a microphone. The data capture unit is connected with an interface 21 provided to process the data captured by the unit 20 into a predetermined format arranged to be processed by the bio-engines. A client feature unit 22 is further connected to the interface 22 and is provided for input of client dedicated features. Such features indicate for example particularities for certain users (poor quality of the voice, etc.) Which can then be taken into account by the device. The data provided by the client feature unit 22 is also formatted by the interface 21.

[0034] The interface 21 is connected to a bio-application program interface 23 which is part of the platform 11. This platform comprises a decision unit formed by a core server 24 and a module manager 25. The decision unit is connected to interface 23. Different bio-engines 26, 27 and 28 are connected to the decision unit and are operating according to a master-slave relationship, the decision unit being the master and the bio-engines the slaves. The module manager 25 is provided for managing the data traffic between the core server and the bio-engines. Bio-engine 26 executes a voice authentication operation and bio-engines 27 and 28 respectively execute a face and a fingerprint authentication. Of course more than three bio-engines could be available and even with two bio-engines the invention could be applicable. It should also be noted that the decision unit can operate on different operating systems, being Windows, Unix etc.

[0035] The decision unit is also connected with a first bio-decision engine 29 provided for executing a serial combinatorial operation with the scores of at least one bio-engine. Bio-decision engine 29 for example can apply an AND operation on the scores of bio-engine 26 or on the scores of bio-engines 26 and 27. The decision unit is further connected with a second bio-decision engine 30 provided for executing a parallel combinatorial operation, i.e. applying an OR operation, with the scores of at least one bio-engine. The first and second bio-decision engines are also slaves for the decision unit. It should be noted that the presence of both the first and the second bio-decision engines is not absolutely required. The device according to the present invention could also operate with only one of those bio-decision engines or even with none of the bio-decision engines.

[0036] A data base manager 31 is also connected to the decision unit. This data base manager controls the data traffic between the decision unit and a database 32 wherein the biometric templates of the clients are stored. A self learning module 33 is further connected to the decision unit and is provided for updating the templates stored in the data base as a result of one or more

good scores issued by the bio-engine. Finally an environmental module 34 to which sensors 35 and 36 are connected, is connected to the decision unit. The latter module is provided for supplying environmental information to the decision unit such as for example background noise which could adversely affect the signal picked up by the microphone, or heavy light intensity which could adversely affect the image recorded by the camera. The sensors 35 and 36 are then formed by a dB meter and a light intensity meter and supply their measurement values to the environmental module 34. The latter then interprets these values and forwards information to the decision unit which thereupon can modify its decision criteria as will be described hereinafter.

[0037] Before the biometric authentication device according to the present invention is fully operative an initialisation process is required. The initialisation process comprises the loading of the client features by means of the client features unit 22. Once loaded they are formatted by the interface 22 and forwarded to the decision unit (24, 25). The biometric templates of the users also have to be created and stored into the database. For this purpose each of the users to who access will be provided to the entity protected by the device, will have to present themselves to the data capture unit so that the necessary data can be collected to form the templates. Once the data capture unit has collected the data from the user, this data is formatted into a biometric template according to a predetermined format by the interface 21 and forwarded via the decision unit and the database manager 31 to the database where the template is stored. If the database stores the templates of several users, a PIN (Personal Identification Number) is assigned to each user and the value of the PIN is stored in the database together with the templates to which the PIN belongs. If a smartcard is used as database the use or manual entry of a PIN is not necessarily required as the user carries this smartcard with him and only needs to insert his smartcard into the device to furnish his template and his supposed identity stored on the smartcard to the device. In order to enable a suitable operation of the device, it is of course necessary that the templates are formatted in a same way as will be the data collected by the data capture unit for an authentication operation.

[0038] The initialisation further comprises the initialisation of the decision unit which is loaded with weight factors to be assigned to the scores issued by the bio-engines as well as the relationship between those weight factors. The threshold value of the device also has to be set, as this will be dependent of the level of security desired.

[0039] The operation of the biometric authentication device according to the invention will now be described with reference to a flowchart shown in figure 9. Suppose a bonafide user wants to get access to an entity protected by the biometric authentication device. The user presents (40) himself in front of the device and types (49) his PIN and/or introduces (41) his smartcard com-

prising his templates. The client module 12 will open (42, 45) an authentication session by activating the data capture unit 20 and reading the introduced PIN and/or the templates available on the smartcard. When a PIN is received the template associated to that PIN is read (46) in the database and supplied to the database manager 32. If the PIN is incorrect, which could be the case with an impostor or due to an error during typing, an error message is generated which can start a retry operation. After a predetermined number of retries, for example threes the device sends a refusal message and access is refused.

[0040] The data capture unit will capture (43) life biometric data from the user, for example by letting him say a predetermined word, for example his name, recording a picture from his face and fingerprint. The captured data is formatted (44) by the interface 21 in order to form a life biometric database which is the supplied (45) to the decision unit.

[0041] The core server of the decision unit is provided to form a decision based on a decision strategy. This strategy comprises the processing of the scores such as issued by the bio-engines 26, 27 and 28. Suppose for example that the Verified Score to be generated by the decision unit is formed by : $V_s = \alpha S_v + \beta S_f + \gamma S_p$ wherein

S_v : score generated by the bio-engine 26 performing the voice authentication

S_f : score generated by the bio-engine 27 performing the face authentication

S_p : score generated by the bio-engine 28 performing the fingerprint authentication

and α , β and γ being weight factors comprised between 0 and 1 and $\alpha + \beta + \gamma = 1$

The scores of the bio-engines being normalized - $1 \leq S \leq +1$

The decision unit will then issue either an acceptance if $V_s > Th$ or a refusal if $V_s \leq Th$, where Th is the threshold value. The values given here are only given by way of example and it will be clear that other values can be used as well as other mathematical relationships for V_s and for the weight factors.

[0042] The life biometric data supplied to the decision unit is forwarded (47) by using the module manager 25 to the respective bio-engines. The module manager also forwards the biometric templates retrieved from the data base to the respective bio-engines. So the voice template and voice life biometric data is forwarded to the bio-engines 26 and respectively the face and the fingerprint data to the bio-engines 27 and 28 respectively. The bio-engines then perform (50) their authentication operation on the received data and generate each a respective score S_v , S_f , S_p .

[0043] Depending on the configuration of the device, the module manager sends the scores to the core server if only one authentication procedure is necessary, or to

the bio-decision engines 29 or 30 if serial or parallel combinatorial operations are requested (48). In the latter case the bio-engines will again perform one or more authentication operations in function of how much attempts are involved in the serial an/or parallel combinatorial operation. In case of combinatorial operations the module manager preferably supplies new life biometric data captured by the data capture unit. The bio-decision engines then perform (51) their combinatorial operation on the scores of the bio-engines and determine a value for S_v , S_f and S_p which is supplied via the module manager to the core server.

[0044] Once the core server has received the score values, the verified scores V_s is determined and compared with the threshold value Th . If $V_s > Th$ the core server issues (52) an acceptance signal and enables (54) access. If $V_s \leq Th$ the core server either issues a refusal or starts a retry (53) depending on how the latter is configured.

[0045] If the core server is configured for starting a retry operation it will generate a control signal in order to start such a retry operation. Under control of such a control signal the weight factors α , β or γ can then be adjusted and further weight factors α' , β' and γ' are generated. This adjustment is for example done by taking into account the score values and/or the client feature. If for example the client feature indicates that the concerned user has a poor voice quality, the weight factor α is reduced for example by 25 % and the others are increased in order to satisfy the criteria $\alpha + \beta + \gamma = 1$. On the other if the score of the face is for example excellent, i.e. substantially higher than the threshold Th_f for the face, and the one of the voice is normal whereas the one of the fingerprint is bad, for example because the finger is injured or burned, the core server can decide to lower γ and increase β . The core server then determines again V_s by using the further weight factors and not necessarily by starting a new authentication process. If $V_s > Th$ an acceptance signal is generated. If not again a retry (53) can be generated or the process is stopped.

[0046] The original aspect of the present device is thus to move the decision to verify and/or identify a user out of the several single bio-engines and to let them operate as slaves of a decision unit where the final decision is taken based on weighted individual scores. The bio-engine as such can no longer alone decide to accept or reject, because their score value is no longer individually checked against a threshold value. Only the verified score, such as obtained and processed by the decision unit, can decide on accept or reject.

[0047] If the device comprise a self learning module 33, the latter is informed by the core server 24 if a bio-engine issues a very high score. This signifies that probably the life biometric data is of exceptional quality. To that purpose the core server for example generates a second control signal when the score of the considered bio-engine is higher than a further threshold value which

is for example 20 % higher than the threshold of that bio-engine. The self learning module will then ask the module manager to furnish this life biometric data and will substitute the template stored in the database by this life biometric data which will now form the biometric template.

[0048] If the device comprises an environmental module 34, the information generated by that module is furnished to the core server under control of a trigger signal generated by that module. The core server is then provided to modify the weight factors α , β and γ in function of the received information and under control of the trigger signal. For example if a heavy background noise is detected, the dB meter will indicate a high value and the core server can decrease the value of α depending on the measured dB value.

Claims

1. A biometric authentication device provided for managing access to at least one entity, said device being operatively connectable to a database provided for storing biometric templates, said device comprising a set of bio-engines each having an input for receiving said biometric templates and life biometric data originating from a data capture unit provided to collect life biometric data, each of said bio-engines being provided for performing a dedicated biometric authentication operation with said biometric templates and said life biometric data and for generating a score as a result of said authentication operation, characterized in that said device comprises a decision unit connected to said bio-engines and operating according to a master-slave relationship, wherein said decision unit being the master, said decision unit being provided for receiving each of said scores and for assigning a respective weight factor to each of said scores and forming a set of weighted scores therewith, said decision unit being further provided for combining said weighted scores and generating a verified score therewith, said decision unit being also provided for comparing said verified score with a threshold value and for generating an access enable signal as a result of a positive comparison and an access refusal signal as a result of a negative comparison.
2. A biometric authentication device as claimed in claim 1, characterized in that the decision unit is connected with a first bio-decision engine, which is provided for executing a serial combinatorial operation with the scores generated by at least one of said bio-engines, said first bio-decision engine being provided to operate as a slave from said decision unit.
3. A biometric authentication device as claimed in claim 1 or 2, characterized in that the decision unit is connected with a second bio-decision engine, which is provided for executing a parallel combinatorial operation with the scores generated by at least one of said bio-engines, said second bio-decision engine being provided to operate as a slave from said decision unit.
4. A biometric authentication device as claimed in anyone of the claims 1 to 3, characterized in that said decision unit is provided for generating a control signal when said verified score is below said threshold, said decision unit being further provided for determining a set of further weight factors under control of said control signal and assigning them to said scores and generating a further verified score therewith.
5. A biometric authentication device as claimed in claim 4, characterized in that said further weight factors and said weight factors each time satisfy a predetermined relationship.
6. A biometric authentication device as claimed in anyone of the claims 1 to 5, characterized in that said decision unit comprises a core server which is provided for generating said verified score and executing said comparison.
7. A biometric authentication device as claimed in claim 6, characterized in that said decision unit comprises a module manager which is provided for managing data traffic between said bio-engines and said core server.
8. A biometric authentication device as claimed in claim 2 and 6 or 3 and 6, characterized in that said decision unit comprises a module manager, which is provided for managing data traffic between said bio-decision engine and said core server.
9. A biometric authentication device as claimed in anyone of the claims 1 to 8, characterized in that said data capture unit is connected to an interface to which a feature module is connected, said feature module being provided for input of client dedicated features.
10. A biometric authentication device as claimed in anyone of the claims 1 to 9, characterized in that said biometric templates are stored on a memory formed by either a smartcard, a harddisk, a EEPROM or a flash memory.
11. A biometric authentication device as claimed in anyone of the claims 1 to 10, characterized in that said device comprises an interface having an input for receiving said life biometric data from said data capture unit.

ture unit, said interface being provided to format said life biometric data according to a predetermined format.

12. A biometric authentication device as claimed in anyone of the claims 1 to 11, characterized is that said decision unit is connected to a self learning module which is provided for substituting into said database a biometric template by a life biometric data under control of a second control signal generated by said decision unit upon detection of a score issued by a bio-engine which is higher than a further predetermined threshold value.

13. A biometric authentication device as claimed in anyone of the claims 1 to 12, characterized in that said decision unit is connected to an environmental module which is provided for generating a trigger signal, said decision unit being provided to modify the weight factors under control of said trigger signal.

25

30

35

40

45

50

55

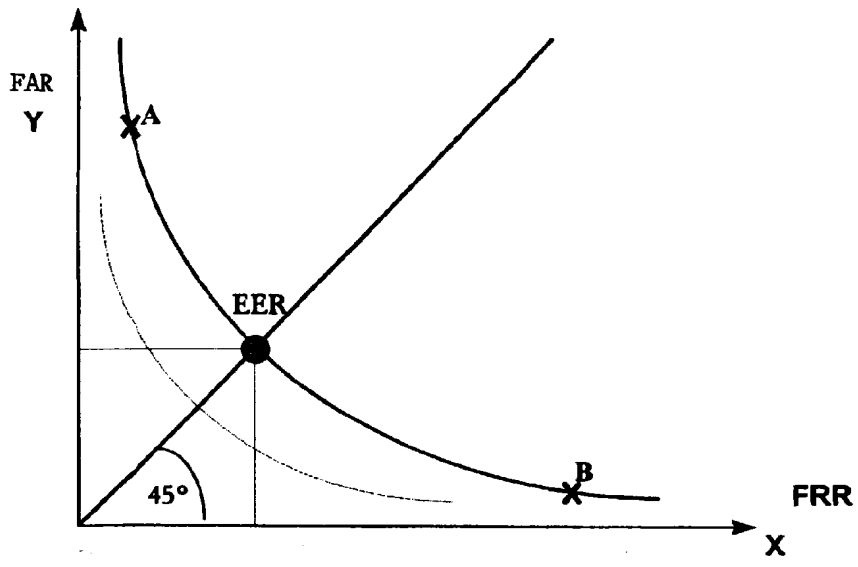


Fig. 1

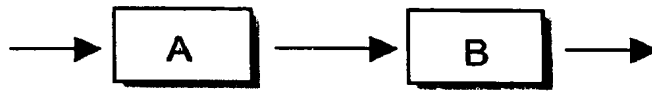


Fig. 2

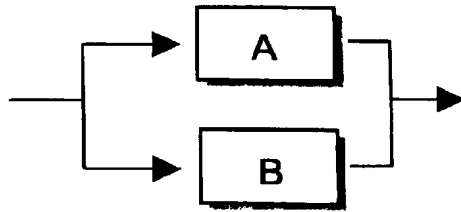


Fig. 3

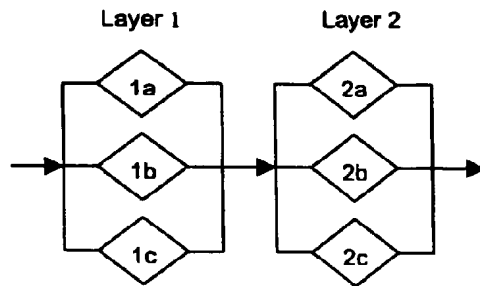


Fig. 4

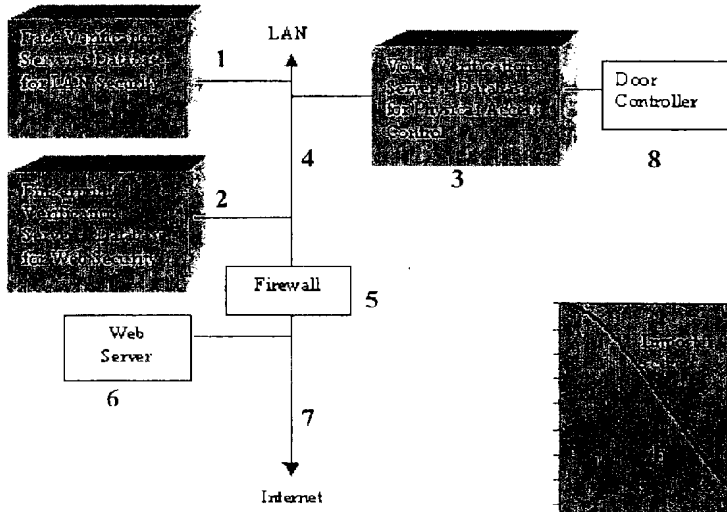


Fig. 5

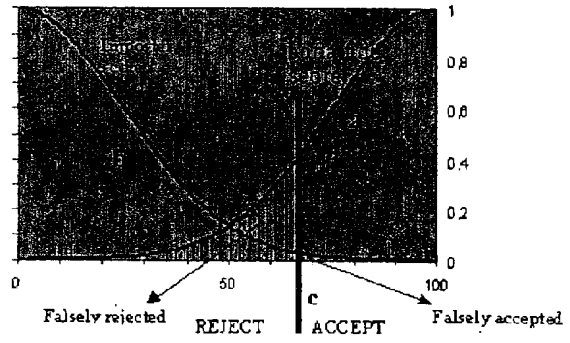


Fig. 6

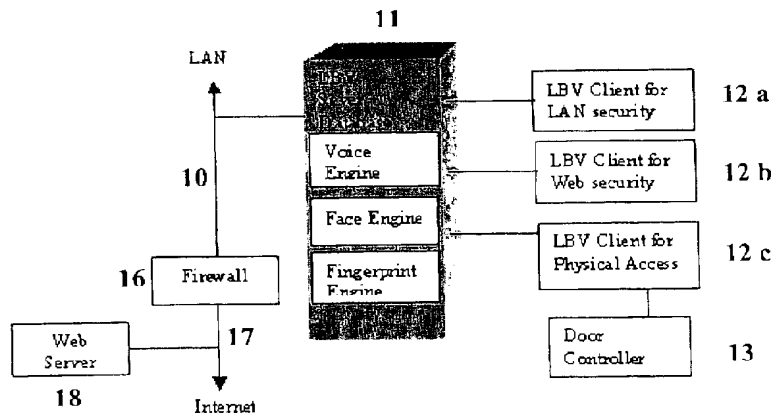


Fig. 7

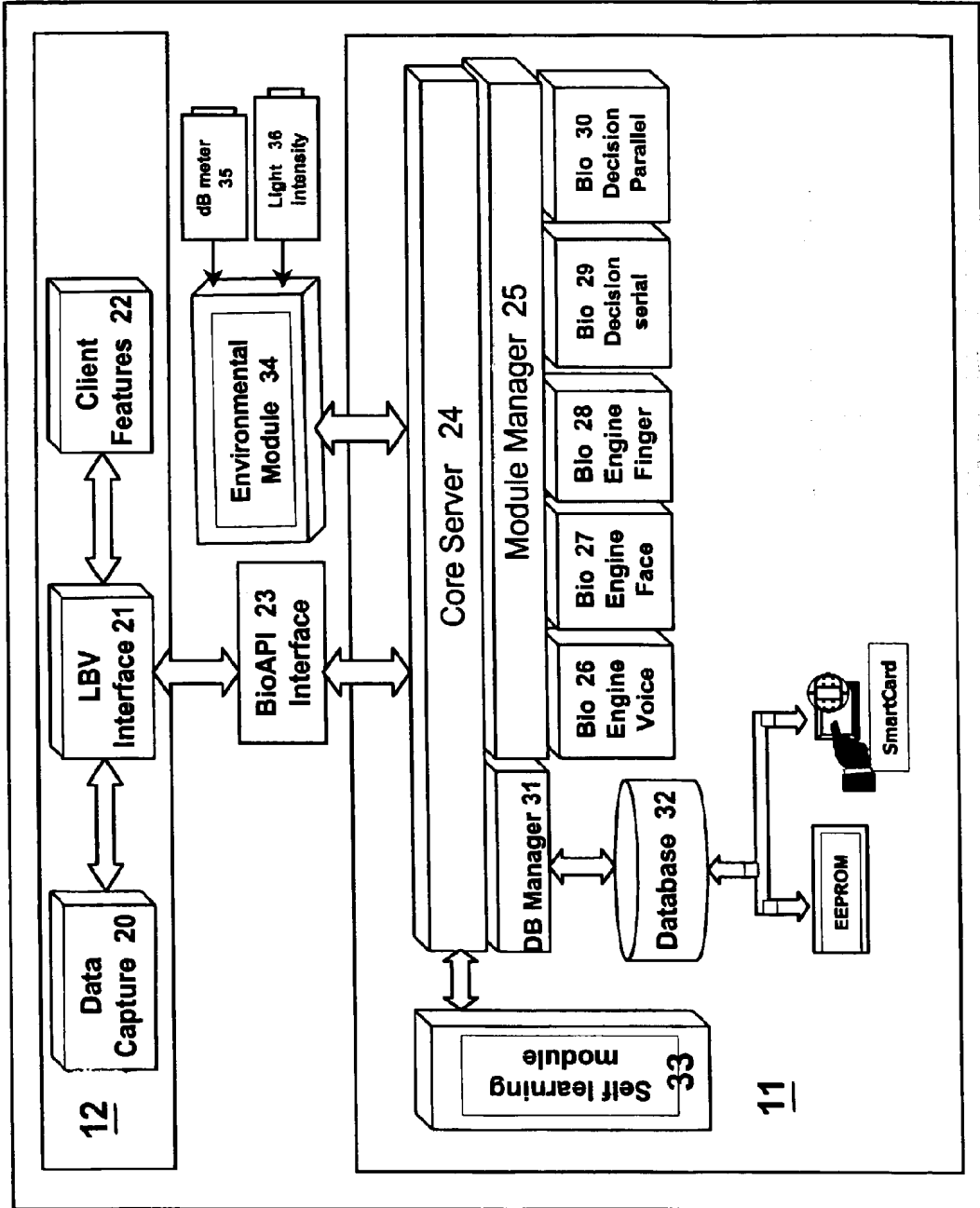
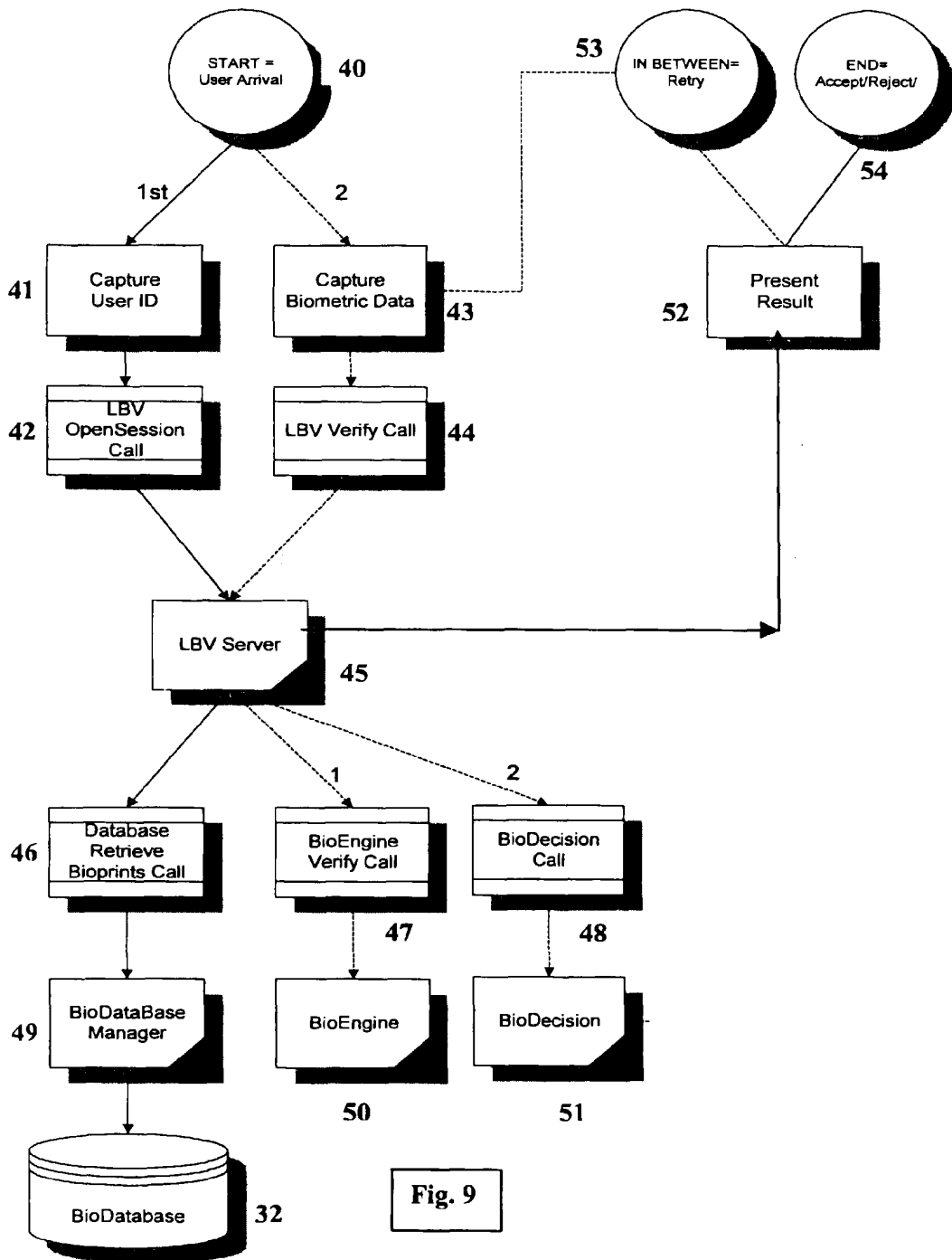


Fig. 8





European Patent
Office

EUROPEAN SEARCH REPORT

Application Number
EP 99 87 0178

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	WO 95 26013 A (MINNESOTA MINING & MFG) 28 September 1995 (1995-09-28) * claim 1; figure 1 *	1-13	G06K9/68
A	LUO R C ET AL: "A TUTORIAL ON MULTISENSOR INTEGRATION AND FUSION" PROCEEDINGS OF THE ANNUAL CONFERENCE OF THE INDUSTRIAL ELECTRONICS SOCIETY. (IECON),US,NEW YORK, IEEE, vol. CONF. 16, 1990, pages 707-722, XP000217315 ISBN: 0-87942-600-4 * the whole document *	1-13	
A	GB 2 229 305 A (BRITISH TELECOMM) 19 September 1990 (1990-09-19) * abstract; figure 1 *	1-13	
A	FR 2 634 570 A (ANDRE CATHERINE ;REITTER RENAUD (FR); REVILLET MARIE JOSEPHE (FR)) 26 January 1990 (1990-01-26) * the whole document *	1-13	
			TECHNICAL FIELDS SEARCHED (Int.Cl.7)
			G06K
The present search report has been drawn up for all claims			
Place of search THE HAGUE		Date of completion of the search 4 February 2000	Examiner Granger, B
CATEGORY OF CITED DOCUMENTS X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document		T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document	

EPO FORM 1503 03/82 (P/4C01)

**ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.**

EP 99 87 0178

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

04-02-2000

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9526013 A	28-09-1995	AU 2186095 A	09-10-1995
		BR 9507142 A	30-09-1997
		CA 2183886 A	28-09-1995
		DE 69501327 D	05-02-1998
		DE 69501327 T	23-07-1998
		EP 0752143 A	08-01-1997
		ES 2110841 T	16-02-1998
		JP 9510636 T	28-10-1997
		US 5719950 A	17-02-1998
		-----	-----
GB 2229305 A	19-09-1990	HK 127496 A	26-07-1996
-----	-----	-----	-----
FR 2634570 A	26-01-1990	NONE	
-----	-----	-----	-----

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

(21) Application No 0126596.6	(51) INT CL ⁷ H04L 9/32
(22) Date of Filing 06.11.2001	(52) UK CL (Edition V) H4P PDCSA
(71) Applicant(s) International Business Machines Corporation (Incorporated in USA - New York) Armonk, New York 10504, United States of America	(56) Documents Cited WO 2001/089133 A1 JP 2001092354 A US 6310966 B1 X.509 Certificates and Certificate Revocation Lists (CRLs), Sun Microsystems, 20 May 1998, http://java.sun.com/products/jdk/1.2/docs/guide/ security/cer t3.html.
(72) Inventor(s) John Owlett Peter Roy Dare	(58) Field of Search UK CL (Edition) H4P PDCSA INT CL ⁷ G06F 1/00, H04L 9/32 29/06 Other: Online: WPI, EPODOC, JAPIO
(74) Agent and/or Address for Service R J Burt IBM United Kingdom Limited, Mail Point 110, Intellectual Property Law, Hursley Park, WINCHESTER, Hampshire, SO21 2JN, United Kingdom	

(54) Abstract Title
Digital certificate containing the identity of an entity which will rely on the certificate

(57) A method and system for supply of data relating to a described entity 302 to a relying entity 304. The method includes generating a first digital certificate referred to as an empowerment certificate signed with an electronic signature by a first signing entity which may be the described entity. The empowerment certificate includes one or more attributes of the described entity 302. The empowerment certificate also includes an indication of data relating to the described entity 302 which is to be supplied and an indication of one or more sources 306 for the data to be supplied. The empowerment certificate also includes one or more attributes identifying one or more relying entities 304 to which the data is authorised to be supplied. The method also includes the relying entity 304 forwarding the empowerment certificate for processing and a source 306 supplying the data indicated in the empowerment certificate. The data relating to the described entity 302 may be supplied to the relying entity 304 by means of a second digital certificate referred to as a custom certificate. The custom certificate is signed with an electronic signature by a second signing entity, preferably the certificate authority 308.

FIG. 3

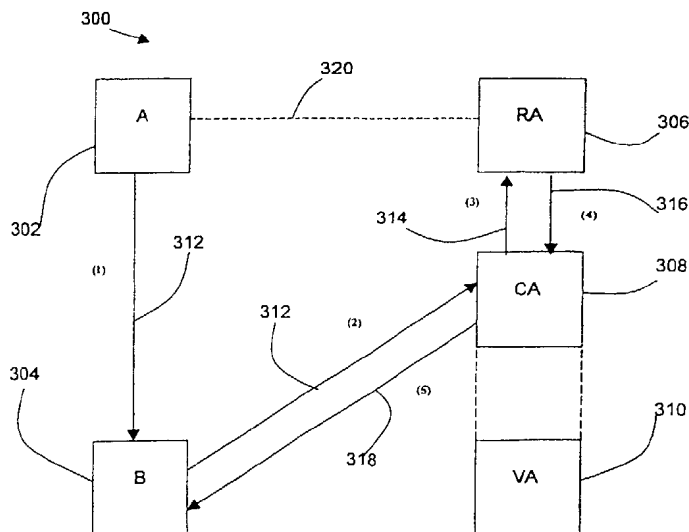


FIG. 1
(PRIOR ART)

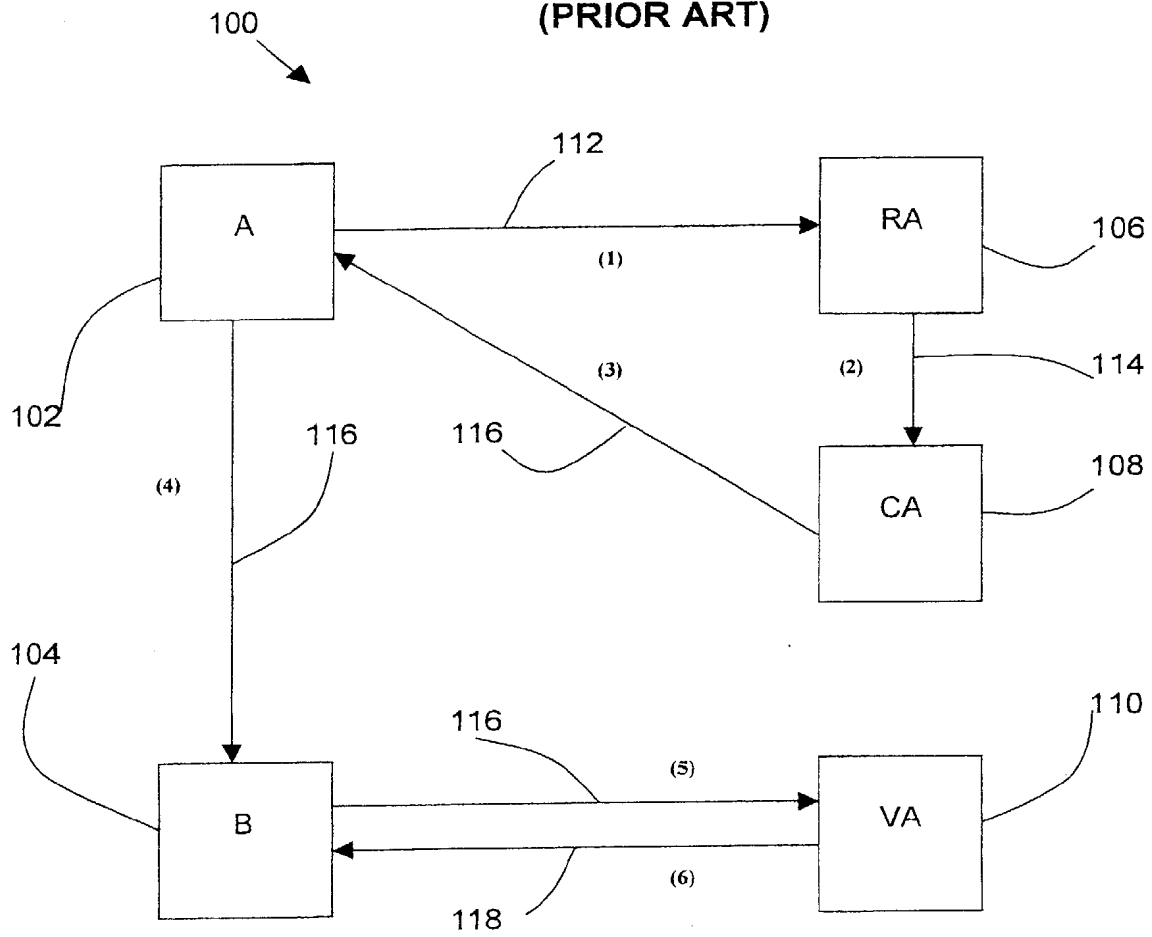


FIG. 2

(PRIOR ART)

200 →

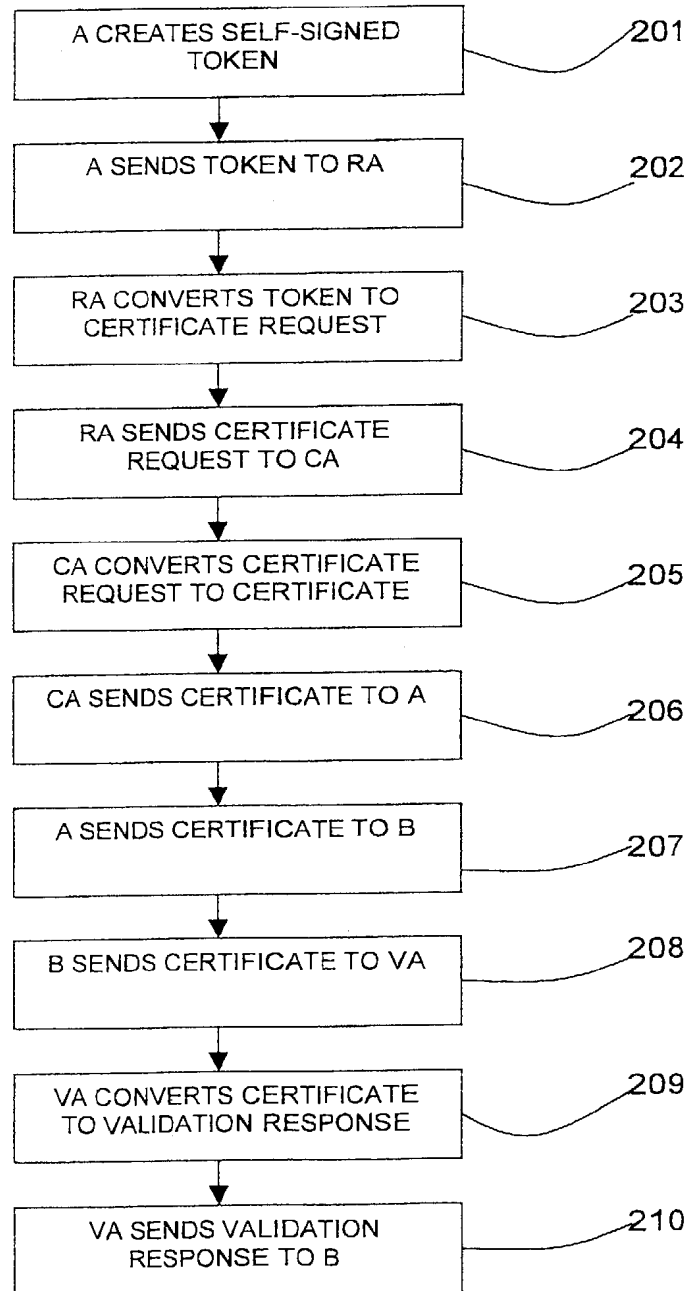


FIG. 3

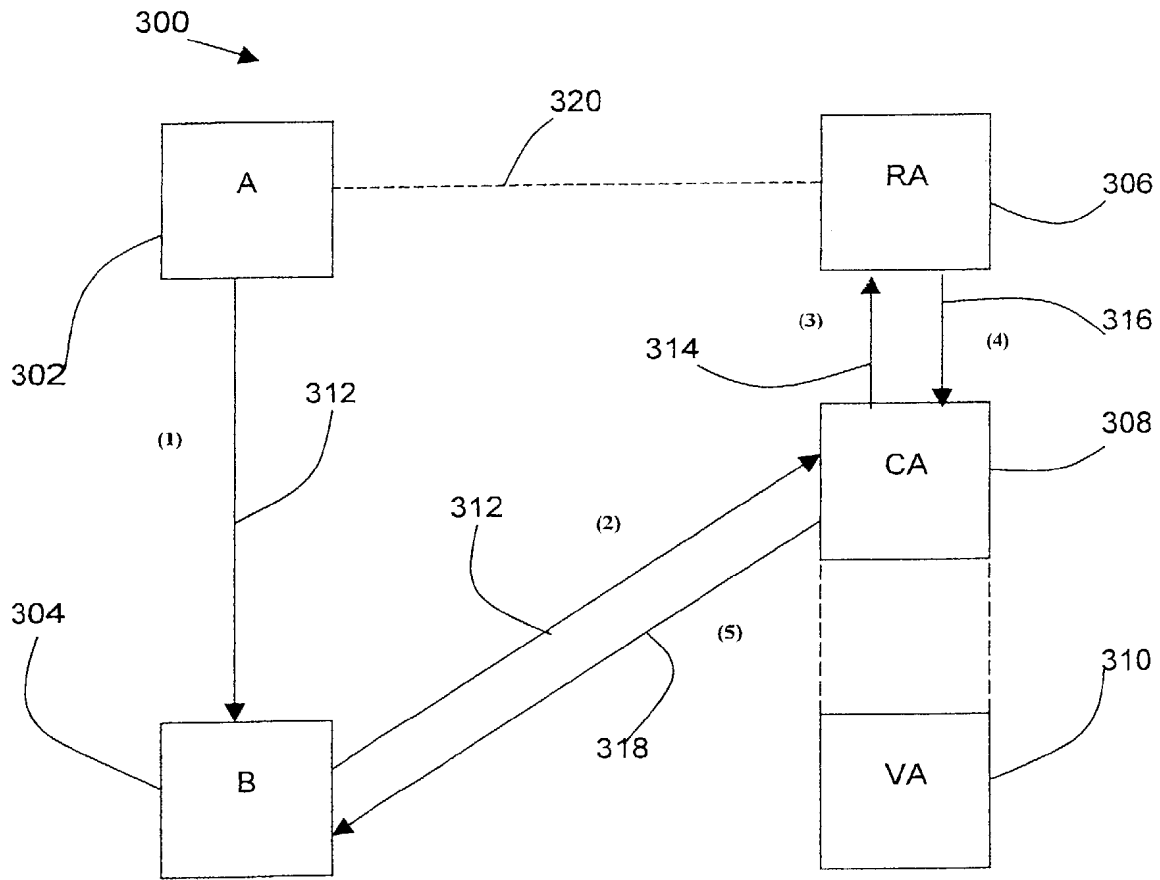
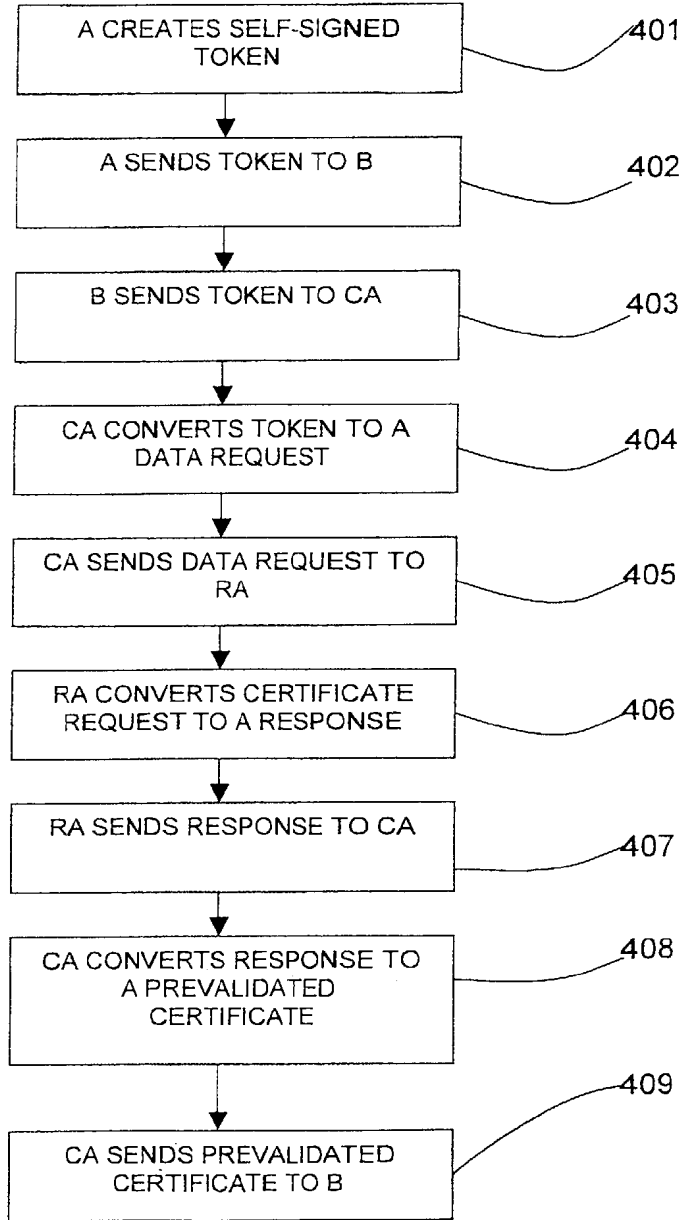


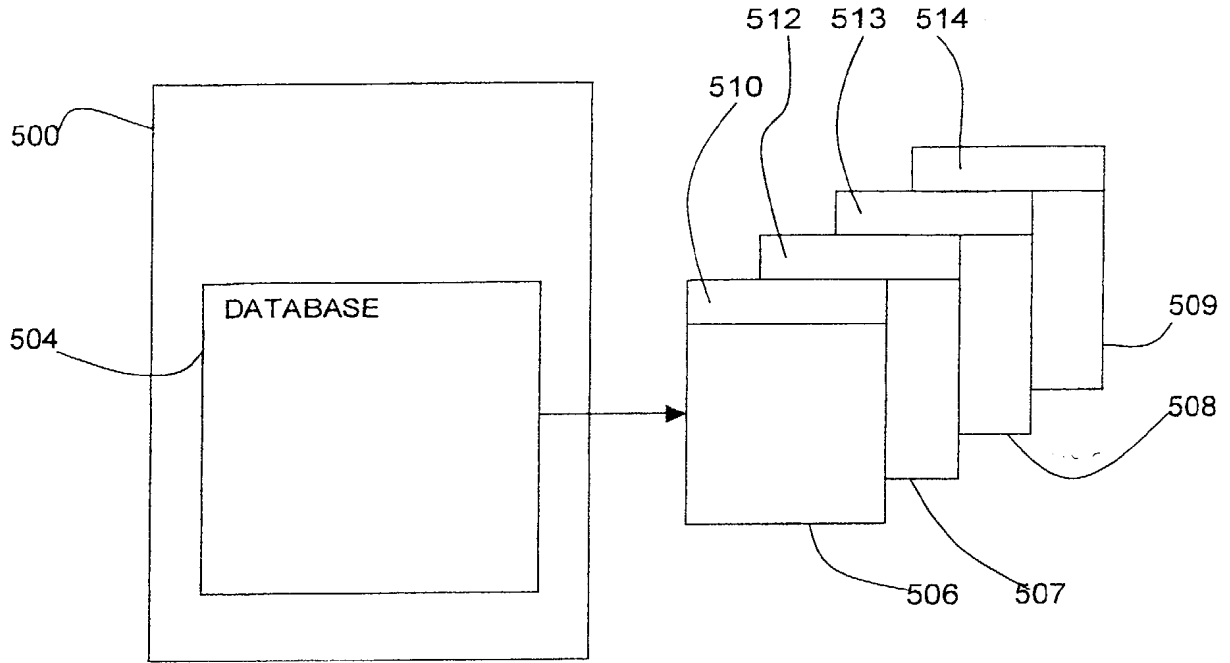
FIG. 4

400



5/7

FIG. 5



6/7

FIG. 6

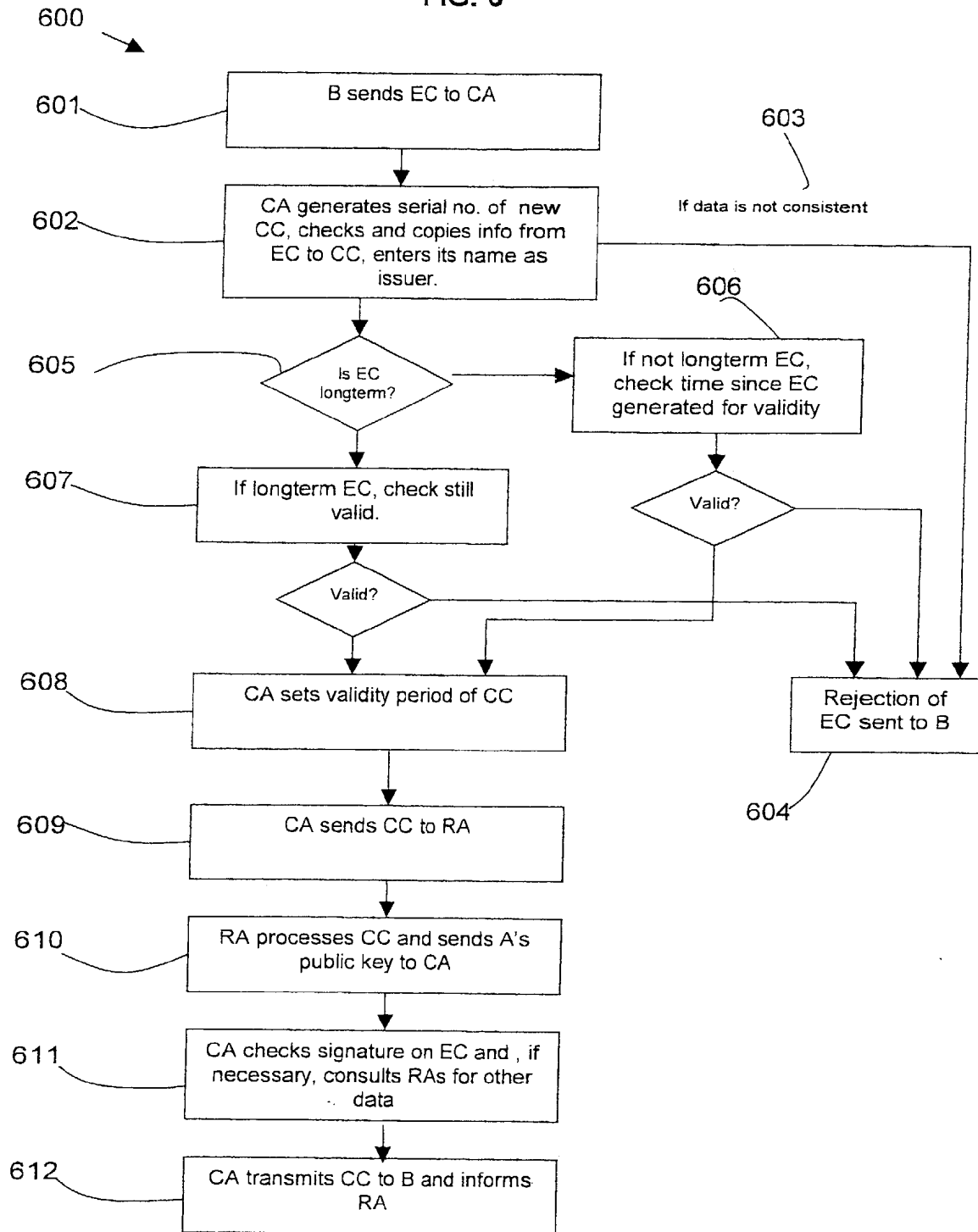
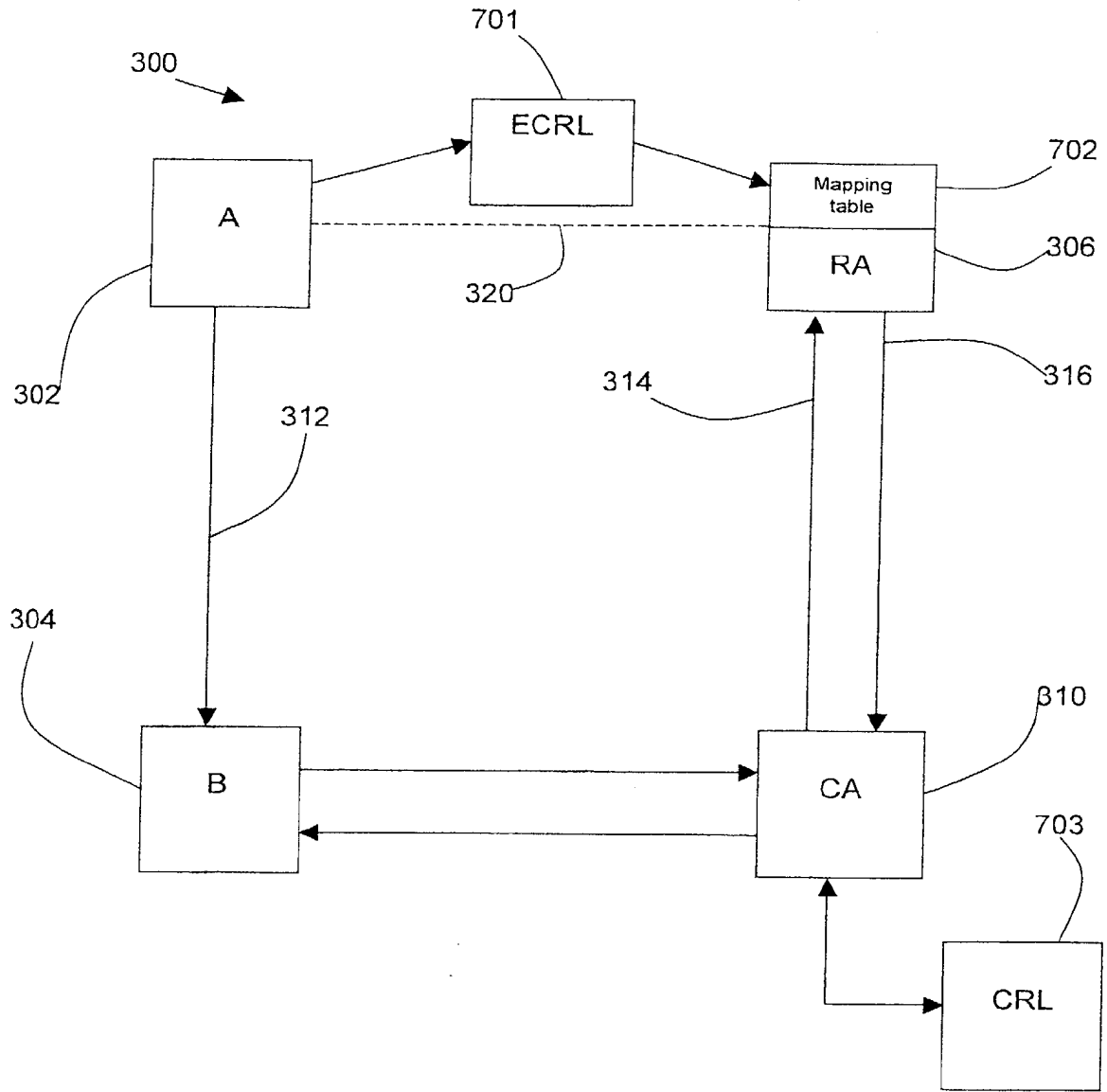


FIG. 7



METHOD AND SYSTEM FOR SUPPLY OF DATA

The invention relates to a method and system for supply of data. This invention also relates to a method for providing a digital signature and digital certificates. The field of the invention is public key cryptography.

Public key cryptography uses an asymmetric algorithm in which the encryption and decryption keys are different and for which it is infeasible to compute one key knowing only the other. Users receive (or, with suitable hardware or software, can generate for themselves) a pair of keys - that is, two large numbers. The user keeps one of these keys private and never discloses it. The other key can be safely made public, just like a phone number or similar personal data. Because of the nature of the algorithm and the way the keys are generated, information encrypted with the private key can only be decrypted with the public key and vice versa. So the sender and receiver do not need to share any secret.

Public key cryptography enables several possibilities:

- Anyone knowing the user's public key can send the user a message encrypted with that key and can be sure that only the user - who alone has the private key - can decrypt it. This provides confidentiality.
- The user might also encrypt a message with his private key. This cannot provide confidentiality, because anyone who knows the public key can decrypt it. But the fact that they can decrypt it means the message must have come from the user - who alone has the private key. This provides integrity and authentication and can also be used as a basis for non-repudiation - the digital equivalent of a signature.
- If a sender signs a message with her own private key and then encrypts it with the recipient's public key, confidentiality, integrity, authentication and non-repudiation are provided together.

In practice, things are actually more complex. In the first example, for performance and operational reasons, the sender will choose a random symmetric session key and use a symmetric cipher to encrypt the message. The public key will be used to encrypt just the session key. Similarly, in the second example, the user will first "digest" the message he wishes to sign, and encrypt the digest with his private key; the recipient will recompute the digest and compare its value with the value he decrypts from the user. A digest is a mathematical construct with a relatively short

fixed length, which is derived from an arbitrarily long message; it has the essential property that it is infeasible, knowing a message and a corresponding digest, to compute another message with the same digest.

5 All the processing is done by software; the real human users do not really "do" any of this.

10 It is important to understand that public keys do not actually have to be published to the world. They can be shared as widely or narrowly as business and privacy requirements dictate.

15 In prior art public keys can be linked together to form a public key infrastructure - a PKI. The links are data structures (or data files) called certificates. Here is how it works:

- Alice may decide to register her public key (and identity information) with a Registration Authority (RA). (In this description of prior art, the usual names "Alice" and "Bob" are used to describe the roles of signatory and relying party, respectively.)
- Using the information collected by the RA, a Certificate Authority (CA) may then create a computer file containing Alice's public key together with information which identifies Alice and a validity period. The CA signs the file with its own private key, creating a certificate.
- A CA's public key may in its turn be certified by another CA; and that CA's certificate will be certified by another and so on until eventually there is a root, that is, an unsigned (or self-signed) public key whose value has to be known some other way.
- So starting from a root it is possible to traverse a certificate chain to discover a public key value.

35 A set of public keys linked in this way form a public key infrastructure. The simplest PKI has a single CA which acts as the root and which signs all the certificates. It is also possible to build a PKI in prior art using cross-certification instead of a hierarchy, but the end result is broadly the same.

40 Anybody with the right software can be an RA or a CA; whatever the legal or business constraints, there is no technical requirement for an authority to be authorised by anybody.

It is important to understand that the linking of a public key into a PKI does not affect what can be done with the matching private key. Some common misconceptions can be clarified as follows:

- 5 • A certificate is "used" by a relying party, not by a holder of a private key. The relying party extracts from the certificate the public key to be used for encryption or signature checking.

- 10 • A certificate is not needed to create a digital signature or to decrypt a received message.

- 15 • A user does not need to be named in any certificate at all to check someone else's signature or to send them an encrypted message.

- 20 • Not even an Advanced Electronic Signature (as defined in the EU Electronic Signatures Directive) requires a certificate to exist in respect of the matching public key.

A typical method in which a PKI is implemented in prior art is as follows.

- 20 • As well as agreeing to look after her private key, Alice applies her ordinary handwritten signature to a paper application form which references "certificate policies" and "certificate practice statements".

- 25 • Alice then constructs and signs a PKCS#10 object which she sends to her RA. PKCS#10 is an industry standard data format.

- 30 • The RA checks the contents of the received object against what it knows about Alice and sends a certificate request to a CA.

- 35 • The CA signs, and sends to Alice, a certificate upon which any Bob in the world can rely. The certificate will probably have an expiry date a year or so in the future. Alice might have to remember to take action to renew the certificate when it expires, perhaps again using a handwritten signature for that purpose.

- 40 • When Alice digitally signs anything, her software sends the certificate to the relying party along with her signature block and the object that has been signed.

- When Bob receives the transmission, he (that is, his software) first examines the certificate, and checks that it is within its period of validity. If he recognises the "issuer", and knows the issuer's public key, he can also check the signature on the certificate. If it computes, he can extract the public key from the certificate and check the signature on the data that was signed.
- Except, of course, that he might not know the public key of the issuer. He now needs a chain of certificates which link to a public key that he does know. Perhaps Alice sent him the chain, or perhaps he has to search public directories to assemble it himself. He may or may not have to pay a charge to access a directory. Bob needs to process the chain by checking that the issuer name in one certificate is the same as the subject name in the next, that all the signatures on all the certificates check out, and that the validity periods within the chain make sense relative to each other. There is a possibility, of course, that no chain can be constructed which includes both the original certificate and a certificate signed by any public key he knows implicitly.
- Except, of course, that the original certificate, or any of the certificates in the chain, may have been revoked. So Bob's software must now go in turn to an Internet address (URL - Uniform Resource Locator) included in each certificate, extract the most recent certificate revocation list (CRL) from that URL, and check that the serial number of the next certificate in the chain does not appear. He may or may not have to pay a charge for access to each CRL.
- As an alternative to the last three bullets, Bob can instead pass the certificate to a validation authority (VA) which will do much of the work for him, and return to him a signed go/no-go response on the validity of the original certificate. If validation services are sufficiently integrated, they may be able to succeed more often than Bob alone could. Use of a validation service will probably be chargeable.
- Bob archives the certificate of interest and either the rest of the chain and the CRLs or the signed validation response. To guard against later revocation of Alice's certificate, Bob would also do well to get from a timestamp authority a timestamp of the signature block on the signed data to prove that he had it in his possession before the revocation occurred.

Ever since the invention of public key cryptography, the vision has been held out of a universal infrastructure that would enable everyone in the world to verify with assurance the digital signatures of everyone else. Electronic transactions exploiting this infrastructure would acquire the important properties of integrity and non-repudiation.

Achievement of the vision would empower individuals because they could digitally sign anything, anywhere, any time. And it would consequently deliver business competitiveness - a typical company, already participating in one e-marketplace as a buyer perhaps, could smoothly enter another, perhaps as a seller, with the same identity. This vision has the potential to alter the nature - and the economics - of the e-marketplace concept. The whole world could develop rapidly into a single e-marketplace - an integrated e-economy.

The prior art does not easily enable subjects to participate in a public key infrastructure with an ability to sign anything, anywhere. Key-pairs in the prior art are generally seen as part of a "managed identity" rather than an extension of personality, independent of certification.

The prior art PKI is largely relevant only in a managed identity context in which a subject is related directly with a single affiliate and the identity only makes sense within that context. For example, an affiliation as an employee, as a customer of a bank, or as a vendor to a major corporation etc. Having acquired or generated a key-pair, the subject convinces a single business partner (a bank, for example, or an employer, or a major customer) of the binding of the subject's identity to its public key. Any particular individual would be likely to have multiple managed identities outstanding at any one time.

A further major problem with the prior art in delivering the universal infrastructure vision is that the CA's contract is typically with the subject and not with the relying party. There is a realisation among traditional CA businesses that the subject will be unwilling to pay the full cost - or perhaps any part of the cost - of "being issued with a certificate".

There is a furthermore a perverse liability issue which arises from the fact that the CA's contract is with Alice - the subject named in the certificate - and not with Bob - who relies on its correctness. In prior art PKI any per-certificate liability is unbounded, because whoever signed the certificate never gets to know who is relying on it until there is a problem. Alice can send the same certificate to a million Bobs and the CA will never know how much liability is building up. The "value" of a

certificate can be reused and reused without the CA (the source of that value) ever becoming aware.

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures ("the Directive") defines a number of the terms used in the present document. However, the definition of "certificate" is wider in the present document than in the Directive; the Directive's use of this word corresponds to the use in the present document of the term "verification certificate". The term "digital signature" in the present document is a technique for implementing the Directive's notion of an "advanced electronic signature".

According to a first aspect of the present invention there is provided a method for supply of data relating to a described entity to a relying entity comprising: generating a first digital certificate signed with an electronic signature by a first signing entity and including: one or more attributes of the described entity; one or more attributes of the first digital certificate which include one or more attributes identifying the first signing entity; an indication of data relating to the described entity which is to be supplied; an indication of one or more sources for the data to be supplied; and one or more attributes identifying one or more relying entities to which the data is to be supplied; the relying entity forwarding the first digital certificate for processing; a source supplying the data indicated in the first digital certificate.

The first digital certificate empowers the relying entity to gain access to the personal data of the described entity which may be held by a source in a data store and may be referred to in this document as an empowerment certificate. The described entity and the relying entity may be individuals, groups of individuals, individuals in a particular role, corporations, organisations, computer applications or systems, automated machines, etc.

Electronic signatures are defined in the Directive as data in electronic form which is attached to or logically associated with other electronic data and which serves as a method of authentication.

The first digital certificate may include any data which the relying entity has previously requested to be included such as a reference, nonce or other data.

A source can hold data or can refer to one or more data sources.

The first digital certificate may be sent with an object signed with a digital signature, but could also be sent on its own. The signing entity

of the first digital certificate may be the described entity such that the first digital certificate is a form of self-signed certificate. If an object signed with a digital signature is sent with the first digital certificate, the digital signature and the electronic signature in the first digital certificate may use different key pairs for signing.

The data relating to the described entity may include one or more public keys corresponding to private keys controlled by the described entity.

The data relating to the described entity may be supplied by means of a second digital certificate to the relying entity, the second digital certificate signed with an electronic signature by a second signing entity and including: one or more attributes of a described entity including the data which is to be supplied; one or more attributes of the second digital certificate which include one or more attributes identifying the second signing entity; and one or more attributes identifying one or more relying entities to which the data is to be supplied.

The second digital certificate may be referred to in this document as a custom certificate. The first and second digital certificates may be in the format prescribed by international and industry standards for certificates with the electronic signature using public key cryptography. The first and second digital certificates may include attributes which are sufficient to identify the described entity as well as the relying entity. These may be a single attribute or a combination of more than one attribute. For example, a name may not be sufficient to identify uniquely an entity, whereas a combination of a name, a date of birth and an address will often uniquely identify the entity.

The first digital certificate may authorise the relying entity to use the first digital certificate to obtain a second digital certificate. The relying entity may be authorised to obtain a second digital certificate which is marked as qualified. "Qualified certificates" are defined in the Directive.

The second digital certificate may include one or more attributes of the first digital certificate. At least some of the contents of the first digital certificate may be copied to the second digital certificate.

The method may include the relying entity forwarding the first digital certificate to an intermediate entity to obtain data from a source. The intermediate entity may provide a service for the relying entity and may provide insurance and take financial liability for the supply of the data

from the source. The intermediate entity may generate the second digital certificate.

5 The second digital certificate may include one or more attributes identifying the relying entity which are different from the one or more attributes identifying the relying entity included in the first digital certificate.

10 The second digital certificate may include one or more attributes identifying the described entity which are different from the one or more attributes identifying the described entity included in the first digital certificate.

15 The described entity may generate a digital signature using a private key with a corresponding public key and the first signing entity may include the digital signature or a cryptographic digest thereof in the first digital certificate and the data to be supplied to the relying entity may include the public key. A cryptographic digest may be obtained using a hash function. Once the indicated data, including the public key, is
20 received by the relying entity from the source, the digital signature can be verified.

25 The first digital certificate and the second digital certificate may include a period of validity. The period of validity of the first digital certificate or the second digital certificate may be that short period of time during which a digital signature was generated. For example, this may be 1 or 2 seconds. A digital certificate can be generated with a validity period which begins prior to the generation of the digital certificate. The period of validity may be in the past, prior to the generation of the
30 digital certificate, or in the future or for a period spanning the past and the future.

35 The data indicated in the first digital certificate may include confirmation of a payment or a debt due from the described entity identified in the first digital certificate to the relying entity identified in the first digital certificate. A second signing entity may indicate in a second digital certificate a guarantee of a debt indicated as due in a first digital certificate.

40 A change in previously supplied data may be indicated by the supply of a list identifying a second digital certificate relating to the previously supplied data. A list may identify a first or second digital certificate specifying data which is no longer authorised to be supplied to the relying entity. The generation of the list may include one or more attributes

identifying relying entities to which the list relates. The list may be a certificate revocation list.

5 The method may include generating and storing a list for the second digital certificates, which is indexed by one or more attributes identifying relying entities such that all second digital certificates in the list relevant to a relying entity can be identified.

10 According to a second aspect of the present invention there is provided a system for supply of data relating to a described entity to a relying entity, the system comprising: a first signing entity application, a relying entity application and a data store wherein the data store holds data relating to the described entity; the first signing entity application has means for generating a first digital certificate signed with an
15 electronic signature by the first signing entity application and including: one or more attributes of the described entity; one or more attributes of the first digital certificate which include one or more attributes identifying the first signing entity; an indication of data relating to the described entity which is to be supplied; an indication of one or more
20 sources for the data to be supplied; and one or more attributes identifying one or more relying entities to which the data is to be supplied; the relying entity application has means for forwarding the first digital certificate for processing; and means for supplying the data indicated in the first digital certificate from the data store.

25 The system may be provided using a secure messaging system across a network, for example the Internet. The described entity and the relying entity may use software applications to generate and sign messages and certificates. The data to be supplied may be held in a data store by a
30 source and the data store may be an electronic database. A source may hold the data store or may refer to one or more further sources. The first signing entity may be the described entity. The system may include more than one data store holding data relating to the described entity.

35 The first digital certificate may include any data which the relying entity has previously requested to be included such as a reference, nonce or other data.

40 A second digital certificate may be provided for supplying the data relating to the described entity to the relying entity application, the second digital certificate signed with an electronic signature by a second signing entity application and including: one or more attributes of the described entity including the data which is to be supplied; one or more attributes of the second digital certificate which include one or more

attributes identifying the second signing entity; and one or more attributes identifying one or more relying entities to which the data is to be supplied.

5 The first digital certificate may authorise the relying entity to use the first digital certificate to obtain a second digital certificate. The relying entity may be authorised to obtain a second digital certificate which is marked as qualified. The second digital certificate may include one or more attributes of the first digital certificate. At least some of the contents of the first digital certificate may be copied to the second
10 digital certificate.

The system may include an intermediate entity application to which the relying entity application forwards the digital certificate to obtain data from the data store. The intermediate entity may use a software
15 application to act between the relying entity and a source. An intermediate entity application may generate the second digital certificate.

20 The second digital certificate may include one or more attributes identifying the relying entity which are different from the one or more attributes identifying the relying entity included in the first digital certificate.

25 The second digital certificate may include one or more attributes identifying the described entity which are different from the one or more attributes identifying the described entity included in the first digital certificate.

30 The described entity may generate a digital signature using a private key with a corresponding public key and the first signing entity may include the digital signature or a cryptographic digest thereof in the first digital certificate and the data to be supplied to the relying entity may include the public key. A cryptographic digest may be obtained using a hash function. Once the indicated data, including the public key, is
35 received by the relying entity from the source, the digital signature can be verified.

40 The first digital certificate and the second digital certificate may include a period of validity. The period of validity of the first digital certificate or the second digital certificate may be that short period of time during which a digital signature was generated. A digital certificate can be generated with a validity period which begins prior to the generation of the digital certificate. The period of validity may be in

the past, prior to the generation of the digital certificate, or in the future or for a period spanning the past and the future.

5 The data indicated in the first digital certificate may include confirmation of a payment or a debt due from the described entity identified in the first digital certificate to the relying entity identified in the first digital certificate. A second signing entity may indicate in a second digital certificate a guarantee of a debt indicated as due in a first digital certificate.

10 A change in previously supplied data may be indicated by the supply of a list identifying a second digital certificate relating to the previously supplied data. A list may identify a first or second digital certificate specifying data which is no longer authorised to be supplied to the relying
15 entity. The generation of the list may include one or more attributes identifying relying entities to which the list relates. The list may be a certificate revocation list.

20 The data store may have a means of determining for an item of data included in the data store information concerning or contained in a first digital certificate which has referenced that item, or information concerning or contained in a second digital certificate which provides the value of that item. The certificate lists just described may be generated through this means.

25 The intermediate entity application may include a storage means for storing second digital certificates referenced by the relying entities identified in the second digital certificates.

30 The system may include a proxy entity application to which the relying entity application or the intermediate entity application may forward the first digital certificate to obtain information specifying to which data store or other proxy entity application the first certificate should next be forwarded.

35 According to a third aspect of the present invention there is provided a computer program product stored on a computer readable storage medium, comprising computer readable program code means for performing the steps
40 of: generating a digital certificate signed with an electronic signature by a signing entity and including: one or more attributes of a described entity; one or more attributes of the digital certificate which include one or more attributes identifying the signing entity; either an indication of data relating to the described entity which is to be supplied and an indication of one or more sources or the data itself; and one or more

attributes identifying one or more relying entities to which the data is to be supplied.

5 A computer program product may be provided with one or more of the features of the first and second aspects of the present invention.

10 According to a fourth aspect of the present invention there is provided a digital certificate signed with an electronic signature by a signing entity and comprising: one or more attributes of a described entity; one or more attributes of the digital certificate which include one or more attributes identifying the signing entity; either an indication of data relating to the described entity which is to be supplied and an indication of one or more sources or the data itself; and one or more attributes identifying one or more relying entities, wherein the relying entities are entities to which the data relating to the described entity is to be supplied.

15 The digital certificate identifying the relying entity may be authorising the relying entity to obtain the indicated data relating to the described entity or may be supplying the data itself to the relying entity.

20 The digital certificate may be provided with one or more of the features of the first and second aspects of the present invention.

25 According to a fifth aspect of the present invention there is provided a method of providing a digital signature based on a digital certificate comprising: generating a digital signature using a private key corresponding to a public key, the signed data including: one or more attributes identifying a digital certificate to be generated; generating a digital certificate signed with an electronic signature by a signing entity and including: one or more attributes of a described entity which are sufficient to obtain the public key; one or more attributes of the digital certificate which include one or more attributes identifying the signing entity; and an indicated period of validity of the digital certificate which begins earlier than the time of generation of the digital certificate; wherein the digital certificate is generated after the generation of the digital signature.

30 An object may be signed with a digital signature which forward references a digital certificate which has not yet been generated and then a digital certificate may be generated which references back to the digital signature and has a period of validity which includes the time of the generation of the digital signature.

More than one digital signature may be generated which identifies the same digital certificate. The signing entity may be the described entity.

5 The period of validity of the digital certificate may be that short period in which the digital signature was generated.

10 The one or more attributes identifying the digital certificate to be generated given in the digital signature may include a serial number. The lowest available serial number which can be used for the next digital certificate to be generated or the last used serial number using each private key may be recorded.

15 According to a sixth aspect of the present invention there is provided a system for providing a digital signature based on a digital certificate, the system comprising:

20 a described entity application with means for generating a digital signature using a private key corresponding to a public key, the signed data including: one or more attributes identifying a digital certificate to be generated; a signing entity application having means for generating a digital certificate with an electronic signature and including: one or more attributes of a described entity which are sufficient to obtain the public key; one or more attributes of the digital certificate which include one or more attributes identifying the signing entity; and an indicated period of validity of the digital certificate which begins earlier than the time of generation of the digital certificate; wherein the digital certificate is generated after the generation of the digital signature.

30 A system may be provided with one or more of the features of the fifth aspect of the present invention.

35 According to a seventh aspect of the present invention there is provided a computer program product stored on a computer readable storage medium, comprising computer readable program code means for performing the steps of: generating a digital signature using a private key corresponding to a public key, the signed data including: one or more attributes identifying a digital certificate to be generated; generating a digital certificate signed with an electronic signature by a signing entity and including: one or more attributes of a described entity which are sufficient to obtain the public key; one or more attributes of the digital certificate which include one or more attributes identifying the signing entity; and an indicated period of validity of the digital certificate which begins earlier than the time of generation of the digital certificate; wherein the digital certificate is generated after the generation of the digital signature.

A computer program product may be provided with one or more of the features of the fifth aspect of the present invention.

5 According to a eighth aspect of the present invention there is provided a digital certificate signed with an electronic signature by a signing entity and comprising: one or more attributes of a described entity; one or more attributes of the digital certificate which include one or more attributes identifying the signing entity; and an indicated period of validity of the digital certificate which begins earlier than the time of generation of the
10 digital certificate.

The indicated period of validity of the digital certificate may end no later than the time of generation of the digital certificate such that the period of validity of the digital certificate is all in the past.

15 Alternatively, the period of validity may extend from the past to a future time.

The described entity may be the signing entity such that the digital signature is a form of self-signed certificate. The electronic signature
20 may use public key cryptography. The digital certificate may include a time stamp indicating the time of generation.

According to a ninth aspect of the present invention there is provided a digital signature using a private key corresponding to the public key
25 derived from a digital certificate as defined in the eighth aspect of the present invention, wherein the digital certificate is generated after the generation of the digital signature, the signed data including: one or more attributes identifying the digital certificate to be generated.

30 The proposed "empowerment infrastructure" which can be implemented through the invention describes a public key infrastructure (PKI) in the sense that it provides for a relying party to establish the value of a public key matching the private key held by an identified subject, and in the sense that it extends the prior art constructs of PKI, including certificates and
35 certificate revocation lists (CRLs) signed by certificate authorities (CAs). The invention itself relies on public key cryptography, but fundamentally challenges the conventional wisdom about the role of keys and certificates in a workable PKI model.

40 The empowerment approach that the invention enables goes well beyond the possibilities of PKI prior art to allow a wide range of personal data items - not just public keys - to be certified within a privacy enhancing framework that empowers the subject to control who can access his personal data, and how and when. The invention enables a method of delivering, not

just public keys, but any piece of assured personal data. In other words, an architecture for an e-marketplace which brings together the buyers and sellers of personal data. The brokers of this marketplace are the data subjects themselves; no personal data moves in the empowerment
5 infrastructure except with the explicit authorisation of the subject to whom that data relates.

The invention also provides a payments mechanism integrated into the personal data framework. Imagine the sale, empowered by Alice, of a piece
10 of personal data of the form "Alice is indeed able to pay you the sum of 100". Usually, when personal data is sold, the database from which it is derived is not altered. But this case has to be an exception, and some database attribute, controlled by the seller of Alice's personal
15 information, has to be altered by exactly - or, where commission or interest are involved, approximately - one hundred. It now just takes a small leap of imagination to see a payment as simply a piece of personal data that changes when it is sold. So the invention also permits a secure
20 payments architecture. By extension, it is also possible to use the infrastructure to confirm a debt due from the signatory to the relying party, and even to indicate a guarantee for such a debt.

Embodiments of the invention are now described, by means of examples only, with reference to the accompanying drawings in which:

25 Figure 1 is a diagram of a system of delivery of data of the prior art;

Figure 2 is a flow diagram of the system of Figure 1;

30 Figure 3 is a diagram of a system of delivery of data in accordance with the present invention;

Figure 4 is a flow diagram of the overall system of Figure 3;

35 Figure 5 is a diagrammatic representation of part of the system in accordance with the present invention;

Figure 6 is a flow diagram of part of the system of Figure 3; and

40 Figure 7 is a diagram of a system in accordance with the present invention.

Referring to Figure 1, the traditional system of delivery of a data object in the form of a certificate as known from the prior art is shown. Figure

1 shows a first user of the system, Alice 102, and a second user, Bob 104. There are also provided a registration authority (RA) 106, a certification authority (CA) 108 and a validation authority (VA) 110.

In the prior art system, the data object to be delivered is a certificate for use in public key cryptography. In public key cryptography, a public key certificate associates a public key value with the certificate's subject. The certificate's subject is a particular person, role, device or other entity that controls the corresponding private key.

A public key certificate is digitally signed by a person or entity called a certification authority.

A registration authority (RA) traditionally manages interactions between a certification authority (CA) and its subscribers or certificate applicants. There may be multiple RAs for a CA. The issuance of a certificate may involve a personal presence for verifying the applicant's identity through presentation of identifying documents. The RA does not itself issue the certificates but may validate, approve or reject certificate applications.

In prior art, the method of delivering a certificate starts with Alice's self-signed token (PKCS#10) 112. PKCS#10 defines a format for a message to request the issuance of a certificate from a CA. The PKCS#10 token 112 allows the requesting entity, Alice 102, to supply her public key and other values requested for inclusion in the certificate. Alice 102 sends the token 112 to the RA 106, which converts it to a certificate request 114. The certificate request is sent by the RA to the CA 108. The CA 108 converts it to a certificate 116 which it sends to Alice 102. Alice 102 sends the certificate 116 unchanged to Bob 104. Bob then sends the certificate unchanged to a validation authority (VA) 110, which converts it to a validation response 118 to Bob 104. Figure 1 shows the order of these actions in numbers given in parentheses.

Figure 2 shows a flow diagram of the traditional system 200 of the prior art described above. Alice creates a self-signed token in the first step 201 and sends this 202 to an RA. The RA converts the token to a certificate request 203 and sends 204 the certificate request to a CA. The CA converts the certificate request to a certificate 205 and sends 206 the certificate to Alice. Alice sends 207 the certificate to Bob. Bob need to have the certificate validated so he sends the certificate to a VA 208. The VA converts 209 the certificate to a validation response either confirming or denying that the certificate is valid. The validation response is sent by the VA to Bob 210.

In a described embodiment of the present invention, a method and system are referred to as an empowerment method or system. This system is shown in Figure 3 using the same structure as Figure 1 for comparison purposes. The embodiment is described in terms of delivery of a certificate for use in public key cryptography; however, as will become evident, the present invention is not restricted to the delivery of certificates only for this particular use. Alice 302 is a described entity and Bob 304 is a relying entity.

Referring to Figure 3, Alice 302 has previously registered 320 with an RA 306 and the RA 306 has information about Alice 302. Alice 302 sends a self-signed token 312 to Bob 304. Bob 304 sends the token 312 unchanged to a CA 308. The CA 308 converts the token to a request 314 to one (or more) RAs 306. The RA 306 converts the request to a response 316 to the CA 308. The CA 308 converts it to a pre-validated certificate 318 which it sends to Bob 304. As the certificate is pre-validated, Bob 304 does not need the explicit services of a VA to validate the certificate. The functions of the VA 310 are combined with the CA 308. Figure 3 shows the order of these actions by numbers in parentheses.

The method 400 of the described embodiment is shown in a flow diagram in Figure 4. In the first step 401 Alice creates a self-signed token. Alice sends 402 the token to Bob. Bob sends 403 the token to a CA. The CA converts 404 the token to a data request and sends 405 the request to a RA. The RA converts 406 the request to a response and sends 407 the response to the CA. The CA converts 408 the response to a pre-validated certificate and sends 409 the pre-validated certificate to Bob.

The traditional system of the prior art and the described embodiment of the system both execute three conversions. Both systems start with Alice self-signing a token and end with Bob possessing a validated certificate naming Alice as subject. But the Alice-to-Bob portion is the first of five steps in the empowerment system of the described embodiment and the fourth of six steps in the traditional system.

This difference of sequence turns out to have far-reaching consequences. In the empowerment system 300, Alice 302 can choose at the granularity of each transaction which of her identities (as employee, taxpayer, bank customer, pseudonym, ...) to assert and which of her attributes (items of personal data) to empower her RA 306 - or RAs - to disclose. Since Bob 304 is now in the customer role with the CA 308, the certificate policy reflects what he is willing to pay, enabling an improved PKI business model in which liabilities are understood and controlled. Because there is no requirement for a certificate to exist before Alice makes her first ever

signature, she can sign her RA agreement digitally rather than in handwritten form.

5 The empowerment system 300 shifts mindset away from the notion of a certificate as part of a managed identity towards a mechanism through which a data subject (Alice 302) empowers an RA to reveal validated personal data to a relying party (Bob 304). A public key value becomes just another piece of validated personal data delivered through this process.

10 The empowerment system of the described embodiment is now considered in more detail.

15 THE DATABASE

The described embodiment of the empowerment system assumes that personal data is held in databases at one or more sources. (The term database is taken to include directories.) Databases model what is going on in the real world. A change in a database reflects a change in the real world.
20 The embodiment only applies to those database entries which identify the subject- that is, where there is sufficient information in the entry to distinguish the subject from all other subjects in that database. There is no requirement that databases must be digital - hardcopy databases are included.

25 Generally, there can be expected to be more than one way to identify a subject. The following is an imagined extract from Alice Earthling's entry in the personnel database of her employer Acme SA:

30 Name

Alice Earthling

35 Date of birth

19631117

Home address

40 65 Southview Road

Employee number

45 65193

Alice's unique number at the Internal Revenue Service (Acme hold this information to pay withholding tax)
DF456781A

5

Alice's banker
Rutland Bank

10

Alice's bank account number (Acme hold this information in order to pay Alice each month)
01081208

15

Alice's work e-mail address
alice.earthling@acme.com

20

Alice's home e-mail address
Alice@earthling.name

25

Alice's work phone number
+99 12 3000 3274

Alice's cellphone number
+99 73 0578 2407

30

Alice's home phone number
+99 13 2553 8109

35

Alice's registered domain name
alice.earthling.name

The value of the public key matching the private key under Alice's control
40 956DF57E4...

A JPEG file containing a full face photograph of Alice
45 AD53827D5C88E575EAB6678...

45

A TIFF file containing a digitised image of Alice's handwritten signature
FE4368AB543C55FDE653FB6...

A pseudonym
756384928475

5

Alice's salary
60,500

10

Alice's external purchasing limit at Acme
100,000

15

The data in the database entry for Alice Earthling includes attributes which provide identification, authentication, location and authorisation. Note that a pseudonym is permitted as an identifier.

20

As the Alice/Acme example includes several data items, it is possible to take several views of the entry, each with a different identifier. So for each view there is a primary identifier and a predicate. The predicate contains all the attributes of the entry except those in the primary identifier which characterise the view. It might be necessary to use a combination of attributes (for example, bank and account number) to construct a single primary identifier, or a single attribute (for example, personnel number) might suffice. In the example, Alice's salary will always be part of the predicate. Her work e-mail address will be part of the predicate in all views except one, namely the view which has her work e-mail address as the primary identifier.

25

30

Note that the possibility of the public key value being a primary identifier is allowed for - making the practical assumption that the same key pair will never be generated twice.

35

This description is for the general case. The system also allows for the simpler case of an entry which has only one possible view because it has only one attribute or set of attributes that could be a primary identifier.

40

THE CERTIFICATE

45

One way of storing data about individuals is in the form of certificates. In the described embodiment, in respect of individuals, a certificate can be seen as a digitally signed extract of an entry in a database. This can

be extended further to include certificates relating to entities that are not individuals. In the described system, certificates are the mechanism through which entries become visible outside the organisation operating each database.

5 A certificate in the described embodiment must contain information from a single view of a single entry. As will be described later, it may also contain other information. This is a crucial difference between a certificate and a database entry. A database entry sits there with all views equally possible. In a certificate, the identifier is committed to a
10 single view.

A certificate must contain the full primary identifier relating to the selected view. The identifier in a certificate is called the "distinguished name". A certificate may also contain information from the predicate of
15 the selected view, either the whole predicate or any sensible subset of it. There little value in a certificate that contains only a distinguished name.

In particular, the predicate information may contain authenticators
20 (including, public key values), locators, authorisers and non-primary identifiers.

Where one or more non-primary identifiers are included, they may be useful as a redundancy checking mechanism. For example, in a certificate which
25 has a bank account number as the primary identifier, one or more of the other identifiers (common name, say) can be used by the bank to double-check against mis-identification.

A traditional certificate known from the prior art identifies a subject or
30 described entity but does not identify any particular relying party or entity. A relying entity is a user of a certificate, that is, someone who relies on the accuracy of the contents of the certificate.

The model's taxonomy then develops as follows:

- 35
- A certificate containing as authenticator a public key which matches a private key used for creating digital signatures is classed as a verification certificate.
 - Verification certificates are either issued to the public, or not, and either qualified or not. The difference is important because the European Union Electronic Signatures Directive treats each class differently.
- 40

• The model assigns certificates to one of three further classes. The classes are traditional, empowerment and custom. Further information on these classes appear later, but in summary:

• A traditional certificate identifies a subject but does not identify any particular relying party. A relying party is a user of a certificate, that is, someone who relies on the accuracy of the contents of the certificate. This class of certificate is found extensively in prior art.

• A custom certificate identifies both a relying party and a subject, and the entity who signs the certificate is not the subject of the certificate.

• An empowerment certificate identifies both a relying party and a subject, and is signed by the subject.

Empowerment and custom certificates are either instantaneous or long term. (Traditional certificates are always long term.) The period of validity of an instantaneous certificate is short enough to practically prevent more than one signature being created in that time with the same private key. It is possible to create many such signatures with the same private key during the period of validity of a long term certificate.

In the model all empowerment and custom verification certificates are classed as issued to the public. In the model custom certificates can be either qualified or unqualified while empowerment certificates can never be qualified.

THE REGISTRATION AUTHORITY

The traditional notion of a registration authority (RA) persists in the described system in the form of sources for data to be supplied. In the embodiment, the registration authority for a given subject is defined as:

- The controller of a database...
- who has agreed with the subject to become an RA in respect of the subject ...
- and includes in its database entry for the subject the value of the subject's public verification key.

In respect of a given subject, an RA is either a direct RA (DRA) or an indirect RA (IRA). The difference is as follows:

5 • A direct RA holds the value of the subject's public key as primary data, updating it in accordance with events in the real world. To achieve this, a DRA probably has some sort of contract with the subject to cover notification in the case of loss or compromise of the corresponding private key.

10 • An indirect RA has cached a longterm custom certificate which contains the value of the public key, and has access to a current certificate revocation list (CRL) which enables the continuing validity of such a certificate to be checked. (CRLs are explained
15 further below.)

The same organisation might be a DRA in respect of one subject and an IRA in respect of another.

20 No subject can have an IRA without also having at least one DRA, although it is possible for a subject to have a DRA and no IRAs. This is because there must be somewhere in the infrastructure where the public key value is bootstrapped. Unless a subject had a DRA in the first place, there could be no longterm custom certificates for any IRA to cache. If a subject
25 stopped having a relationship with its last DRA, then it is likely that all the relevant longterm custom certificates would very soon appear in the CRLs which the IRAs check, so very quickly the subject would cease to have any IRA relationships either.

30 There is nothing in the described system which prevents a subject having more than one DRA - either because the subject has more than one key pair or because one or more key pairs are tracked by one or more DRAs.

35 The mechanism through which the DRA is sure of the subject's public key value is outside the description given here and is not part of the invention. There are however plenty of examples in prior art of how this relationship can be implemented. In fact, any RA - DRA or IRA - has to have some method of establishing the value of all the data items it holds "for real" on each subject, not just the public key. Again, there is a
40 mass of existing prior art in this area. ("For real" means "not in a certificate signed by somebody else".)

The correct operation of this unspecified mechanism is axiomatic to the whole model. Everything that happens elsewhere in the model depends on this part being done correctly.

5 Figure 5 shows a representation of the RA 500 of the described system. The RA holds a database 504. 506, 507, 508, 509 are single views of the database. Each view 506, 507, 508, 509 has a distinguished name 510, 512, 513, 514 for that view which is the primary identifier. The views 506, 507, 508, 509 can also include attributes from the predicate of the
10 selected view of the database, including public key values, locators, authorisers, etc.

In the described system, RAs have the following capabilities.

15 An RA (of either class), in its role as a database controller, can maintain and process the data it holds on each subject for whatever reason it is, apart from being an RA, that it holds that data. So, for example, the personnel department of Alice Earthling's employer Acme will continue to process the monthly payroll against the employee database.

20 An RA (of either class) can receive and process entry updates digitally signed by the subject. The RA knows the subject's public key (either because, as a DRA, it is tracking it or, as an IRA, because it can validate the cached certificate against the CRL), so it is always able to check the signature.

25 Importantly, an RA can send a message to a certificate authority (CA) which can result in the CA signing or revoking a digital certificate.

30 The described system predicts that many organisations - and perhaps most organisations within the public sector - will become RAs. In such cases, being an RA will be incidental to being something else. There is no specific requirement in the system for organisations whose whole business mission is that of an RA, although such organisations are obviously possible.

35 **THE SIGNING DEVICE**

The model abstracts a digital signature to the operation of a finite state machine called a signing device. The signing device has access to a source
40 of local time which corresponds to the usual standards notion of GeneralizedTime and which increments with a granularity of one second. The state of the machine is defined by:

- the value of a key pair, which can change from time to time;
- the value of an empowerment certificate serial number, which is an integer that increases before or after each signature operation; and
- 5 • (optionally) by a set of values that enable intelligent guesses to be made of data to be included in an empowerment certificate.

How the machine and its state are implemented is not defined in the model and are not part of the invention, but it may prove helpful to think of a smart card or a wireless device. There are minor privacy advantages in
 10 incrementing the serial number by amounts other than unity to obfuscate the rate at which Alice is effecting signing operations.

A signing operation might proceed as follows:

- 15 • The device takes the value of the local time.
- The device increments the empowerment certificate (EC) serial number.
- 20 • For each of zero or more objects to be signed in turn it displays each object to Alice, and receives from her a decision whether or not to sign.
- For each object that Alice wants to sign, if any, the device
 25 computes a signature block over a data structure consisting of:
 - the object to be signed;
 - a reference, by serial number and the hash of Alice's
 30 public key value, to the EC about to be created; and
 - possibly other information.
- The device then displays an EC confirmation screen with
 35 intelligent guesses of the values to be included in the EC, together with the EC serial number. These intelligent guesses are computed from information provided externally to the device when it was invoked, and from the internally-held optional values.

• The device builds the EC from the information Alice provided (or accepted from the intelligent guesses) and from the signature blocks of the signed objects. The period of validity of the EC is set to begin at the time taken at the start of the operation (in the first bullet above), and ends one second after the GeneralizedTime recorded at the end of the operation, or, with Alice's approval, a longer period. The device appends Alice's signature to the EC.

10 THE EMPOWERMENT CERTIFICATE

As an alternative to certificates described in prior art, the described system provides for Alice's software to send Bob an empowerment certificate. This alternative mechanism has a number of unique advantages that mean that Alice does not need to be "issued" with a traditional certificate (or, indeed, any digital certificate at all).

Although Alice has not been "issued" with a certificate, her software still transmits a certificate with every object she signs, but it is always a certificate that her software has built for her and that she herself signs immediately after signing the object to be signed. The whole transaction can sometimes be completely encapsulated in the self-signed certificate alone, making the signing of an associated object unnecessary. The described system calls these special self-signed certificates "empowerment certificates".

Empowerment certificates can be seen as a mechanism by which a user empowers others to gain access to their personal data, including their public key which can be considered to be an ordinary piece of personal data.

The generation of an empowerment certificate includes the following steps. The objects to be signed, if any, are signed first, with a forward reference to the empowerment certificate about to be created included in the data to be signed. The empowerment certificate is then created and signed, with a backward reference to the signature blocks of the signed objects (if any).

The following information is contained in an empowerment certificate:

- 1 A distinguished name that Alice asserts as "issuer".
- 2 The same distinguished name as subject.
- 3 The distinguished name of the relying party.

- 4 The distinguished name of an RA who can resolve Alice's distinguished name to a public key value (or to one or more such values).
- 5 .5 A period of validity beginning one second before the time taken at the start of the signing operation and ending no earlier than two seconds after that time.
- 6 (Optionally) a set of attribute definitions.
- 7 For each attribute definition, either an asserted value or the distinguished name of an RA who holds that attribute value for the subject.
- 10 .8 (Optionally) the distinguished name of an RA who holds the particular attribute that is the subject's public key value.
- 9 (If any) the signature block(s) over the previously signed object(s).
- 15 .10 (If any) a random nonce or other information provided by the relying party. A nonce is typically a large number whose value until it is generated is unpredictable.
- 11 (Optionally) the subject's public key or one of the subject's public keys, or a reference to such a key.
- 20 .12 (Optionally) policy information. Alice might include a statement of the purposes for which she agrees that the personal information asserted or referenced in the empowerment certificate may be used, or the purposes for which she states that it may not be used. She may also indicate her approval for the later generation of a custom qualified certificate using the EC.
- 25 .13 The subject's signature over all the above. There are circumstances (basically, those circumstances in which the signature on the empowerment certificate will never be verified) in which the signature can be omitted, but these circumstances are not discussed further.
- 30 Optionally, the model allows for the possibility that one or more of the RAs which hold the data to be provided are referenced indirectly in the empowerment certificate rather than by distinguished name. The EC might identify a proxy service which knows which RA is to be used for each attribute. There is clearly no limit to the amount of such indirection
- 35 (one proxy pointing to another proxy, and so on) which might in principle be implemented.

On receiving the empowerment certificate and any signed object(s) from Alice, Bob has four options:

1. Bob may just simply believe what Alice has asserted, not even bothering to check the signature on the empowerment certificate.

At its simplest, the described system acts as a method of transmitting unauthenticated personal data. If Bob is a government agency and Alice wants to be mailed an information leaflet, then it does not much matter if she is lying about her name and home address. This simple use of the empowerment certificate can also deliver the same sort of benefits as browser cookies.

More usually, if there is an accompanying signed object, Bob may not bother to check the signature on the empowerment certificate if he has a longterm custom certificate cached which contains Alice's public key. He will simply pull Alice's distinguished name from the empowerment certificate, find the relevant longterm custom certificate and extract her public key from there to check the signature on the signed object.

2. Alternatively, Bob may check the signature using an asserted value of the public key and just simply believe the rest of the asserted information (if any) if the signature checks out.

This is of some use because, if Bob caches empowerment certificates, it can provide a session mechanism in applications where key revocation is not important. That is, Bob will associate Alice's first visit to his website with her second and subsequent visits, without necessarily getting to know for sure any of Alice's personal data except her public key value. Bob can prevent replay attacks by supplying a nonce for each visit or by checking for increasing empowerment certificate serial numbers. If Alice asserts some other identifier (even a pseudonym) on any visit, then she need not assert her public key on subsequent visits. This mechanism cannot, however, recover from compromise of Alice's signing device, or from Alice rolling over her key. In the first case, someone else can take over the "session"; in the second case the session ends without the possibility of any in-band explanation to Bob.

Despite its limitations, this mechanism has considerable advantages compared to password-based website logon schemes.

3. Another possibility is that Bob checks the signature on the empowerment certificate using a public key value for Alice that he has cached on a longterm custom certificate or knows in some other way (because he is her DRA, for example).

This provides a method of authentication that can cope with revocation.

Once again, Bob can use a nonce or a serial number check to guard against replays. Bob may also be happy to believe without further assurance the asserted information (if any) in the empowerment certificate that differs from what he already has cached or otherwise knew.

5

This use of empowerment certificates provides a method for subjects to inform RAs of changes they need to make to their databases. Archive of the empowerment certificate provides an audit record signed by the subject.

10

4. Most importantly of all, Bob can use the empowerment infrastructure to convert a properly-signed empowerment certificate into a custom certificate (or, indeed, more than one custom certificate). This is a crucial part of the described system and is explained next. If Bob takes this route, it is prudent for him to check that Alice has correctly copied the object signature block (if any) to the empowerment certificate.

15

THE CUSTOM CERTIFICATE

20

Just as Alice has a contract with one or more RAs, so Bob, if he wants to convert an empowerment certificate into a custom certificate, needs to have a contract with one or more CAs. The process is straightforward. At any time before the expiry of the empowerment certificate (or as soon as possible after the expiry of an instantaneous empowerment certificate), and as many times as he likes, Bob sends to a CA an empowerment certificate which he has received and the CA signs and returns an equivalent custom certificate, customised to Bob's requirements. There are no restrictions in the system on Bob's choice of CA, or on how many times (provided, in the case of an instantaneous empowerment certificate that he is quick), or to how many different CAs he sends the same empowerment certificate.

25

30

What the CA is doing is executing Alice's mandate, given when she created the empowerment certificate, for certain of her personal data to be shared with Bob. Her public key a piece of personal data which may be shared in this way.

35

The following describes the method steps. If anything goes wrong, the process ends and Bob's request is rejected with a reason code.

40

The CA generates the serial number of the custom certificate being prepared and copies the empowerment certificate serial number, the hash of the empowerment certificate, the object signature blocks (if any) and the nonce (if any) as attributes in the custom certificate. The CA copies its own distinguished name into the issuer field along with a timestamp

For a longterm empowerment certificate, the CA checks that the period of validity of the empowerment certificate will not have expired before the time likely to assemble and sign a custom certificate. For an instantaneous empowerment certificate, the CA checks that only a reasonable
5 period of time has passed since the empowerment certificate was signed. "Reasonable" means that Alice's personal data is highly unlikely to have changed since she signed the empowerment certificate.

For both longterm empowerment certificates and instantaneous empowerment
10 certificates (for which the reasonable period has not passed), the CA will set the validity period start time of the custom certificate the same as the start time of the empowerment certificate. Otherwise (and this will clearly apply to longterm custom certificates only), the validity period start time will be set to the time by the CAs clock. As an option, to
15 support store-and-forward transactions, it may be useful for the start time to be set to a significantly earlier time.

The custom certificate validity period end time will be set to the empowerment certificate validity period end time, or to an earlier time
20 that Bob specifies.

The CA checks that Bob is named as relying party in the empowerment certificate and names Bob as the relying party in the custom certificate. Within defined rules, certain changes to the presentation of Bob's name is
25 permitted. (The analogy here is the flexibility with which banks match payee names on cheques to accountholder names.)

The CA checks that the empowerment certificates subject name and "issuer" name are identical and copies the value into the subject field of the
30 custom certificate. Again, within defined rules, changes to Alice's name are permitted.

The CA ignores (that is, treats as if they were not present) any attribute in the empowerment certificate that has been asserted rather than
35 referenced to an RA. Asserted attribute values in empowerment certificates have benefit in the part of the communication between Alice and Bob not involving a CA. Asserted public key values do have one use within the infrastructure. which is explained below.

The CA then presents the empowerment certificate to the RA identified in the empowerment certificate as able to resolve Alice's distinguished name into her public key. If this is a longterm empowerment certificate, the RA will first check to see if Alice has revoked it. How the RA does that is explained later. (The instantaneous or longterm status of the custom

certificate is irrelevant.) In any case, the RA checks the validity period of the empowerment certificate.

5 The RA consults its database, extracts the value of the public key and checks the empowerment certificate. If it knows of more than one public key for Alice it will try each in turn, guided by hints she has included in the empowerment certificate (for example, asserting the value of, or the value of the hash of, a public key), until the signature on the empowerment certificate checks out.

10 For a longterm custom certificates only, the RA adds, to each of the attributes that compose the distinguished name, a label of the following form ("DN flag", CA's distinguished name, custom certificate serial number, expiry date). No label is added for an instantaneous custom certificate.
15 (The instantaneous or longterm status of the empowerment certificate is irrelevant for this decision.)

20 The RA examines the empowerment certificate to see if it is named as the RA for any of the predicate attributes, including the public key. It pulls out of its database any values that Alice has empowered. For a longterm custom certificate only, the RA adds to each attribute a label of the form ("att flag", CA's distinguished name, custom certificate serial number, expiry date). No label is added for an instantaneous custom certificate.
25 (The instantaneous or longterm status of the empowerment certificate is irrelevant for this decision.)

30 For longterm custom certificates, the RA caches the empowerment certificate, and records the mapping of empowerment certificate and custom certificate serial numbers, expiry dates and "issuers".

The RA sends the following information back to the CA:

.14 Alice's public key value.

.15 The values of any predicate attributes for which it is responsible.

35 If a public key value is included among the predicate attributes and Alice has more than one public key, the RA will choose one on the basis of the public key value or hash value that Alice asserted. This may or may not be the same value as the public key value returned above, because Alice might approve with a signature using one private key the creation of a custom
40 certificate containing the public key corresponding to another of her private keys.

The CA is now able to check the signature on the empowerment certificate, and does so. If there are any more RAs to be consulted, the CA sends out the empowerment certificate in parallel to them, along with the first public key value returned by the first RA. The RAs check the empowerment certificate, including again its expiry and revocation status, use the distinguished name in the empowerment certificate, or the public key value, to identify the subject, and return the values. As before, for longterm custom certificates they label "att flag" attributes, cache the empowerment certificate and map the empowerment certificate to the custom certificate.

Note that the public key to be included in a public key custom certificate may be provided by an RA other than the RA who initially resolved Alice's distinguished name into her public key.

With all the attribute information back, the CA now marks the certificate to indicate the certificate policy that Bob has requested. In particular, if Bob has asked for a qualified certificate, and the CA is happy that this is possible, the CA marks the certificate as qualified, with a liability limitation the lower of what Bob has requested and what the CA is willing to offer. The policy Alice set in the EC will also constrain whether or not a custom qualified certificate can be generated.

To get the policy and liability he wants, Bob can even submit the empowerment certificate independently to two or more CAs, or to the same CA multiple times, playing off the weakness in one policy with the strength of another, to use one custom certificate to reinforce another, or to spread a qualified certificate liability over two or more CAs.

There is one important constraint on the policy that the CA defines in the custom certificate. Any personal data policy limitations that Alice defined in the original empowerment certificate are carried forward into the custom certificate.

Finally, the CA informs the RA who resolved Alice's distinguished name into her public key the fact of transfer to Bob of the custom certificate. The CA will provide the serial numbers of the empowerment certificate and longterm custom certificate, and say whether the longterm custom certificate is qualified or not (so that Alice knows if her signature was upgraded to qualified status as defined in article 5.1 of the EU Electronic Signatures Directive). The RA is specifically not told anything else about the policy, and is not told the amount of any liability limitation. (It is none of Alice's business what value Bob attaches to his relationship with her.)

Bob obviously has an option to ask for only a subset of the possible predicate attributes to be included.

5 Figure 6 shows a flow diagram of the method 600 carried out by the CA. The method 600 starts with the empowerment certificate being sent by Bob to the CA 601. At step 602, the CA generates a serial number for the new custom certificate, checks that the data of the empowerment certificate is consistent and copies the data into the custom certificate and enters its name as the issuer of the custom certificate. If any data is inconsistent
10 603, the empowerment certificate is rejected and returned to Bob 604.

The CA checks the validity of the empowerment certificate by first ascertaining if the certificate is instantaneous or longterm 605. If the empowerment certificate is instantaneous, the time since it was generated is checked to make sure this is within a predetermined time 606. If the
15 empowerment certificate is longterm, the validity period is checked 607. If the empowerment certificate is outside its validity period, the empowerment certificate is rejected and returned to Bob 604.

The CA then sets the validity period of the custom certificate 608 and
20 sends the custom certificate to the RA 609. The RA processes the custom certificate and sends Alice's public key to the CA 610. The CA checks the signature of the empowerment certificate with the public key 611. If some of the data referred to in the empowerment certificate is held in other RAs the CA will send requests to the other RAs for the data. The CA signs the
25 custom certificate and transmits it to Bob 612. The CA also informs the RA that the data has been sent to Bob.

THE CUSTOM CERTIFICATE REVOCATION LIST

30 Just as the system provides for custom certificates, so too there are custom certificate revocation lists. They apply to longterm custom certificates only, because instantaneous custom certificates expire within a second of their generation, so the question of their revocation never
35 arises.

Through a mechanism that is about to be explained, a CA will become aware of any change to information included in a longterm custom certificate that it has signed, provided that the change occurs before the expiry of the longterm custom certificate concerned. Also, Alice can at any time revoke
40 any of the empowerment certificates she has signed, which means that the corresponding longterm custom certificates must also be revoked. Bob can also ask for any longterm custom certificate in which he is named as relying party to be revoked.

A CA maintains a separate custom certificate revocation list (CRL) for each of its customers, and each customer only gets to see its own CRL. Bob can consult his CRL anytime he wishes, can specify the normal frequency he
5 wants CRLs updated, and can even force the creation of a new CRL at any time. Bob can also be asked to be notified each time a new CRL is available for his inspection. Bob can archive CRLs so that he can later prove that a particular longterm custom certificate was unrevoked at any particular time.

10 Whenever a certificate serial number appears in a CRL, Bob will want to archive the revoked certificate. If the empowerment certificate that matched the revoked longterm custom certificate is still unexpired, then Bob can resubmit the matching empowerment certificate and try to get a new
15 longterm custom certificate with updated content. Whether he is successful or not depends on the reason for revocation, and Bob can see the revocation reason code in his CRL.

20 Clearly, if Alice revoked the empowerment certificate, then no way is the infrastructure going to yield up a longterm custom certificate to Bob. Alice has withdrawn that particular empowerment to her personal data. And a longterm custom certificate will not be recoverable if Alice's distinguished name is deleted.

25 If only the value of an attribute or a public key has changed, or if Alice has simply changed the way her personal data is allocated to RAs, then the empowerment certificate can usually be resubmitted and a replacement longterm custom certificate obtained, valid for the remaining duration of the empowerment certificate.

30 Bob can request a longterm custom certificate at any time before the empowerment certificate expiry. Bob can even contract with the CA for the CA to automatically process a new request every time a revocation occurs, without Bob needing to start the exercise off. And Bob can present the
35 same empowerment certificate to different CAs during its lifetime.

40 So, as Alice rolls over her key pair, or changes her name on marriage, or receives an increased purchasing limit from Acme, or changes bank, or moves house, or changes phone number, or even changes employer, the longterm custom certificates around the world which name her as subject will quickly get revoked and replaced. Bob's address book will always be up to date. Alice needs to tell just one of her RAs of her change of circumstances, and everyone she has empowered to know about those circumstances will very soon know what has happened. This applies to every piece of data in unexpired

longterm custom certificates - identifiers, predicate, authenticators, authorisers, locators.

5 Every time a CA revokes a longterm custom certificate it flags the serial number of the revoked longterm custom certificate to the RA who resolved Alice's distinguished name into her public key.

The following describes how the method works in detail.

10 Alice is optionally able to maintain, through her software functionality, constructs known as empowerment certificate revocation lists (ECRLs). At any time she can present to any of her RAs an ECRL listing the serial numbers of previously-generated longterm empowerment certificates still valid that she wishes to revoke. (Instantaneous empowerment certificates expire shortly after their creation, so the question of their revocation never arises.)

15 When any of the RAs receives an ECRL, it extracts from the list the serial numbers of all the empowerment certificates which it has processed for Alice, looks at its mapping table to find the matching CA names and custom certificate serial numbers, and sends signed messages to each CA instructing revocation on the grounds of "empowerment certificate revocation".

25 If a particular empowerment certificate names more than one RA, Alice can send the ECRL to any one of them. This provides her with the ability to revoke a part of an empowerment certificate, at the granularity of the RA. It is even possible to allow revocation at the granularity of an attribute. There is a requirement for a revocation code "partial empowerment certificate revocation".

- 30 • If Alice decides to move an item of her personal data from one RA to another, the RA will look at the labels on that item of data, extract the serial numbers of unexpired custom certificates and send signed revocation messages to the relevant CAs, with a reason code "change of RA".
 - 35 • Every time a piece of Alice's data changes value in its database, the RA will examine the labels attached and will send out signed revocation messages for each custom certificate. For custom certificates where the DN flag is set, the revocation reason will be "identity deleted". Where the att flag is set, the reason will be "attribute change".
- 40

- Finally, if, through methods not defined in the system, an RA learns of the death of a subject, it will cause the revocation of all that subject's unexpired custom certificates with a reason code "death of subject".

5

It is worthwhile resubmitting unexpired empowerment certificates only if the revocation reason was "partial empowerment certificate revocation", "change of RA" or "attribute change".

10

Figure 7 shows the diagram of Figure 3 with the addition of the certificate revocation lists. An empowerment certificate revocation list 701 is transmitted by Alice 302 to the RA 306. The RA 306 has a mapping table 702 in which a record of all empowerment certificates and custom certificates is kept with reference to their serial numbers and a record of the CAs to which the data has been supplied. The RA 306 can inform the CAs of any custom certificates which should be revoked further to a revocation request from Alice 302. The CA 310 keeps a certificate revocation list 703 for each relying entity such as Bob 304.

15

20

THE INFRASTRUCTURE

25

The empowerment infrastructure consists of a secure (that is, signed and encrypted) messaging and transaction system linking a set of RAs and CAs which offer empowerment services to their customers. Methods of implementing such transaction systems are well described in prior art.

30

As the CAs and RAs communicate securely among themselves, they in turn could exploit the same mechanisms as we have shown Alice and Bob to exploit.

35

Improvements and modifications can be made to the foregoing without departing from the scope of the present invention.

CLAIMS

5 1. A method for supply of data relating to a described entity (302) to a
 relying entity (304) comprising:
 generating a first digital certificate signed with an electronic signature
 by a first signing entity and including:
 10 (one or more attributes of the described entity (302));
 one or more attributes of the first digital certificate which include
 one or more attributes identifying the first signing entity;
 an indication of data relating to the described entity (302) which is
 to be supplied;
 an indication of one or more sources (306, 500) for the data to be
 15 supplied; and
 one or more attributes identifying one or more relying entities (304)
 to which the data is to be supplied;
 the relying entity (304) forwarding the first digital certificate for
 processing;
 20 a source (306, 500) supplying the data indicated in the first digital
 certificate.

25 2. A method as claimed in claim 1, wherein a source (306, 500) can hold
 data or can refer to one or more further sources (306, 500).

30 3. A method as claimed in claim 1 or claim 2, wherein the first signing
 entity is the described entity (302).

35 4. A method as claimed in any one of claims 1 to 3, wherein the first
 digital certificate includes a reference, nonce or other data which the
 relying entity (304) has previously requested to be included.

40 5. A method as claimed in any one of claims 1 to 4, wherein some or all
 of the data relating to the described entity (302) is supplied by means of
 a second digital certificate to the relying entity (304), the second
 digital certificate signed with an electronic signature by a second signing
 entity and including:

45 one or more attributes of the described entity (302) including the
 data which is to be supplied;
 one or more attributes of the second digital certificate which
 include one or more attributes identifying the second signing entity;
 and
 one or more attributes identifying one or more relying entities (304)
 to which the data is to be supplied.

6. A method as claimed in claim 5, wherein the first digital certificate authorises the relying entity (304) to use the first digital certificate to obtain a second digital certificate.

5 7. A method as claimed in claim 6, wherein the relying entity (304) is authorised to obtain a second digital certificate which is marked as qualified.

10 8. A method as claimed in any one of claims 5 to 7, wherein the second digital certificate includes one or more attributes of the first digital certificate.

15 9. A method as claimed in any one of claims 5 to 8, wherein at least some of the contents of the first digital certificate is copied to the second digital certificate.

20 10. A method as claimed in any one of the preceding claims, wherein the method includes the relying entity (304) forwarding the first digital certificate to an intermediate entity (308) to obtain data from a source (306, 500).

11. A method as claimed in claim 10, wherein the intermediate entity (308) generates the second digital certificate.

25 12. A method as claimed in any one of claims 5 to 11, wherein the second digital certificate includes one or more attributes identifying the relying entity (304) which are different from the one or more attributes identifying the relying entity (304) included in the first digital certificate.

30 13. A method as claimed in any one of claims 5 to 12, wherein the second digital certificate includes one or more attributes identifying the described entity (302) which are different from one or more attributes identifying the described entity (302) included in the first digital certificate.

35 40 14. A method as claimed in any one of the preceding claims, wherein the described entity (302) generates a digital signature using a private key with a corresponding public key and the first signing entity includes the digital signature or a cryptographic digest thereof in the first digital certificate, and the data to be supplied to the relying entity (304) includes the public key.

15. A method as claimed in any one of the preceding claims, wherein the first digital certificate includes a period of validity.

5 16. A method as claimed in any one of claims 5 to 15, wherein the second digital certificate includes a period of validity.

10 17. A method as claimed in claim 15 or claim 16, wherein the period of validity of the first digital certificate or the second digital certificate is that short period of time during which a digital signature was generated.

15 18. A method as claimed in any one of the preceding claims, wherein the data indicated in the first digital certificate includes confirmation of a payment or debt due from the described entity (302) identified in the first digital certificate to the relying entity (304) identified in the first digital certificate.

20 19. A method as claimed in claim 18, wherein a second signing entity indicates in a second digital certificate a guarantee of a debt indicated as due in a first digital certificate.

25 20. A method as claimed in claims 5 to 19, wherein a change in previously supplied data is indicated by the supply of a list identifying a second digital certificate relating to the previously supplied data.

30 21. A method as claimed in any one of the preceding claims, wherein a list (701, 703) identifies a first or second digital certificate specifying data which is no longer authorised to be supplied to the relying entity (304).

35 22. A method as claimed in claim 20 or claim 21, wherein the generation of the list (701, 703) includes one or more attributes identifying the relying entities (304) to which the list (701, 703) relates.

40 23. A method as claimed in any one of claims 5 to 22, which includes generating and storing a list (703) for the second digital certificates, which is indexed by one or more attributes identifying relying entities (304) such that all second digital certificates in the list (703) relevant to a relying entity (304) can be identified.

24. A system for supply of data relating to a described entity (302) to a relying entity (304), the system comprising:

a first signing entity application, a relying entity application and a data store (504) wherein the data store (504) holds data relating to the described entity (302);

the first signing entity application has means for generating a first digital certificate signed with an electronic signature by the first signing entity application and including:

one or more attributes of the described entity (302);

one or more attributes of the first digital certificate which include one or more attributes identifying the first signing entity;

an indication of data relating to the described entity (302) which is to be supplied;

an indication of one or more sources (306, 500) for the data to be supplied; and

one or more attributes identifying one or more relying entities (304) to which the data is to be supplied;

the relying entity application has means for forwarding the first digital certificate for processing; and

means for supplying the data indicated in the first digital certificate from the data store (504).

25. A system as claimed in claim 24, wherein a source (306, 500) holds the data store (504) or can refer to one or more further sources (306, 500).

26. A system as claimed in claim 24 or claim 25, wherein the first signing entity is the described entity (302).

27. A system as claimed in any one of claims 24 to 26, wherein the first digital certificate includes a reference, nonce or other data which the relying entity (304) has previously requested to be included.

28. A system as claimed in any one of claims 24 to 27, wherein a second digital certificate is provided for supplying the data relating to the described entity (302) to the relying entity application, the second digital certificate signed with an electronic signature by a second signing entity application and including:

one or more attributes of the described entity (302) including the data which is to be supplied;

one or more attributes of the second digital certificate which include one or more attributes identifying the second signing entity; and

one or more attributes identifying one or more relying entities (304) to which the data is to be supplied.

29. A system as claimed in any one of claims 24 to 28, wherein the system includes an intermediate entity application to which the relying entity application forwards the first digital certificate to obtain data from the data store (504).

5

30. A system as claimed in any one of claims 24 to 29, wherein the system includes more than one data store (504) holding data relating to the described entity (302).

10

31. A system as claimed in any one of claims 24 to 30, wherein a data store (504) has a means of determining for an item of data included in the data store (504) information concerning or contained in a first digital certificate which has referenced that item

15

32. A system as claimed in any one of claims 28 to 31, wherein a data store (504) has a means of determining for an item of data included in the data store (504) information concerning or contained in a second digital certificate which provides the value of that item.

20

33. A system as claimed in any one of claims 29 to 32, wherein the intermediate entity application has a storage means for storing second digital certificates referenced by the relying entities (304) identified in the second digital certificates.

25

34. A system as claimed in any one of claims 24 to 33, wherein the system includes a proxy entity application to which the relying entity application or the intermediate entity application forwards the first digital certificate to obtain information specifying to which data store (504) or other proxy entity application the first certificate should next be forwarded

30

35. A computer program product stored on a computer readable storage medium, comprising computer readable program code means for performing the steps of:

35

generating a digital certificate signed with an electronic signature by a signing entity and including:

one or more attributes of a described entity (302);

one or more attributes of the digital certificate which include one or more attributes identifying the signing entity;

40

either an indication of data relating to the described entity (302) which is to be supplied and an indication of one or more sources (306, 500) or the data itself; and

one or more attributes identifying one or more relying entities (304) to which the data is to be supplied.

36) A digital certificate signed with an electronic signature by a signing entity and comprising:

one or more attributes of a described entity (302);

one or more attributes of the digital certificate which include one or more attributes identifying the signing entity;

either an indication of data relating to the described entity (302) which is to be supplied and an indication of one or more sources (306, 500) or the data itself; and

one or more attributes identifying one or more relying entities (304), wherein the relying entities (304) are entities to which the data relating to the described entity (302) is to be supplied.

37. A method of providing a digital signature based on a digital certificate comprising:

generating a digital signature using a private key corresponding to a public key, the signed data including:

one or more attributes identifying a digital certificate to be generated;

generating a digital certificate signed with an electronic signature by a signing entity and including:

one or more attributes of a described entity (302) which are sufficient to obtain the public key;

one or more attributes of the digital certificate which include one or more attributes identifying the signing entity; and

an indicated period of validity of the digital certificate which begins earlier than the time of generation of the digital certificate;

wherein the digital certificate is generated after the generation of the digital signature.

38. A method as claimed in claim 37, wherein more than one digital signature can be generated which identifies the same digital certificate.

39. A method as claimed in claim 37 or claim 38, wherein the period of validity of the digital certificate is that short period in which the digital signature was generated.

40. A method as claimed in any one of claims 37 to 39, wherein the one or more attributes identifying the digital certificate to be generated given in the digital signature include a serial number.

41. A method as claimed in claim 40, wherein the lowest available serial number which can be used for the next digital certificate to be generated or the last used serial number using each private key is recorded.

42. A system for providing a digital signature based on a digital certificate, the system comprising:
a described entity application with means for generating a digital signature using a private key corresponding to a public key, the signed data including:

one or more attributes identifying a digital certificate to be generated;

a signing entity application having means for generating a digital certificate with an electronic signature and including:

one or more attributes of a described entity (302) which are sufficient to obtain the public key;

one or more attributes of the digital certificate which include one or more attributes identifying the signing entity; and

an indicated period of validity of the digital certificate which begins earlier than the time of generation of the digital certificate;

wherein the digital certificate is generated after the generation of the digital signature.

43. A computer program product stored on a computer readable storage medium, comprising computer readable program code means for performing the steps of:

generating a digital signature using a private key corresponding to a public key, the signed data including:

one or more attributes identifying a digital certificate to be generated;

generating a digital certificate signed with an electronic signature by a signing entity and including:

one or more attributes of a described entity (302) which are sufficient to obtain the public key;

one or more attributes of the digital certificate which include one or more attributes identifying the signing entity; and

an indicated period of validity of the digital certificate which begins earlier than the time of generation of the digital certificate;

wherein the digital certificate is generated after the generation of the digital signature.

44. A digital certificate signed with an electronic signature by a signing entity and comprising:

one or more attributes of a described entity (302);

one or more attributes of the digital certificate which include one or more attributes identifying the signing entity;

an indicated period of validity of the digital certificate which begins earlier than the time of generation of the digital certificate.

5 45. A digital certificate as claimed in claim 44, wherein the indicated period of validity of the digital certificate ends no later than the time of generation of the digital certificate.

10 46. A digital certificate as claimed in claim 44 or claim 45, wherein the described entity (302) is the signing entity.

15 47. A digital certificate as claimed in any one of claims 44 to 46, wherein the digital certificate includes a time stamp indicating the time of generation.

20 48. A digital signature using a private key corresponding to the public key derivable from a digital certificate as claimed in claim 44, wherein the digital certificate is generated after the generation of the digital signature,

the signed data including:

25 one or more attributes identifying the digital certificate to be generated.



INVESTOR IN PEOPLE

Application No: GB 0126596.6
Claims searched: 1-36

Examiner: John Cullen
Date of search: 4 October 2002

Patents Act 1977 Search Report under Section 17

Databases searched:

UK Patent Office collections, including GB, EP, WO & US patent specifications, in:
UK CI (Ed.T): H4P (PDCSA)
Int CI (Ed.7): G06F 1/00; H04L 9/32, 29/06
Other: Online: WPI, EPODOC, JAPIO

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
A, E	WO 2001/089133 (SURETY.COM) See Fig. 1 A2	---
A	US 6310966 B1 (GTE SERVICE) See Figs. 1 and 2.	---
A	JP 2001-092354 (NIPPON TELEGRAPH) 6.4.2001 (See PAJ Abstract and WPI Abstract Accession No. 2002-085134/12).	---
A	X.509 Certificates and Revocation Lists (CRLs), Sun Microsystems, 20.05.1998, http://java.sun.com/products/jdk/1.2/docs/guide/security/cert3.html . See section entitled 'What's Inside an X.509 Certificate?'.	---

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.



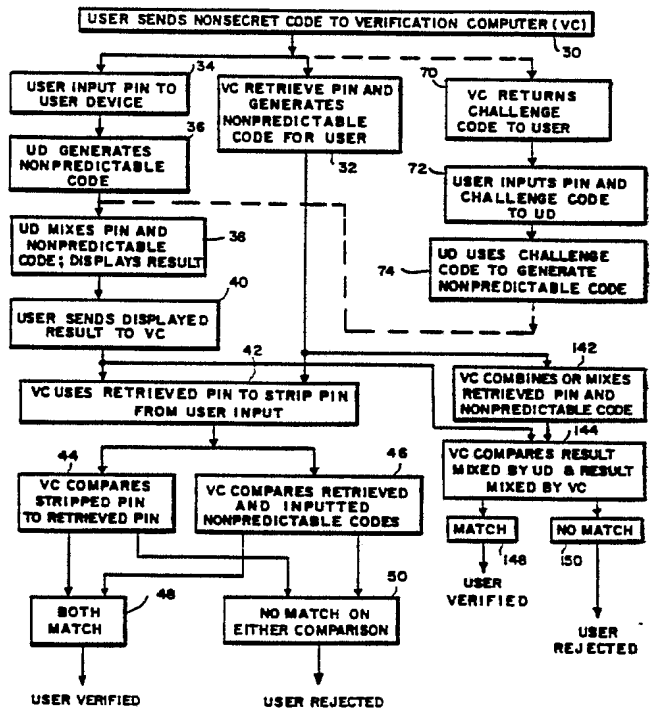
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification 5 : H04K 1/00</p>	<p>A1</p>	<p>(11) International Publication Number: WO 92/07436 (43) International Publication Date: 30 April 1992 (30.04.92)</p>
<p>(21) International Application Number: PCT/US91/03034 (22) International Filing Date: 30 April 1991 (30.04.91) (30) Priority data: 597,784 19 October 1990 (19.10.90) US 670,705 18 March 1991 (18.03.91) US (71) Applicant: SECURITY DYNAMICS TECHNOLOGIES, INC. [US/US]; One Alewife Center, Cambridge, MA 02140-2312 (US). (72) Inventor: WEISS, Kenneth, P. ; 7 Park Avenue, Newton, MA 02159 (US). (74) Agent: OLIVERIO, M., Lawrence; Wolf, Greenfield & Sacks, Federal Reserve Plaza, 600 Atlantic Avenue, Boston, MA 02210 (US).</p>		<p>(81) Designated States: AT (European patent), AU, BE (European patent), CA, CH (European patent), DE (European patent), DK (European patent), ES (European patent), FR (European patent), GB (European patent), GR (European patent), IT (European patent), JP, LU (European patent), NL (European patent), SE (European patent). Published <i>With international search report.</i></p>

(54) Title: METHOD AND APPARATUS FOR PERSONAL IDENTIFICATION

(57) Abstract

A method and apparatus for providing improved security for a personal identification number (PIN) in a personal identification and verification system of the type wherein a time dependent nonpredictable code is generated at a device in the possession of the individual (36), which code is unique to the individual and this code is communicated to, and compared with a nonpredictable code generated at a central verification computer (46). In this system, the PIN is mixed with the nonpredictable code before transmission of these values to the central verification computer (38). A nonsecret code (30) is previously transmitted to the central verification computer and is used by the verification computer to retrieve the PIN and independently generate the time dependent appropriate nonpredictable code for the user (74). These retrieved PIN and generated code values are used by the verification computer either (a) to strip the PIN from the transmitted nonpredictable code (42) and the stripped PIN and remaining nonpredictable code are compared with the corresponding retrieved values in order to determine verification (44, 46); or (b) to be mixed and then compared with the mixed PIN and code which is transmitted to the verification computer (144).



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	ES	Spain	MG	Madagascar
AU	Australia	FI	Finland	ML	Mali
BB	Barbados	FR	France	MN	Mongolia
BE	Belgium	GA	Gabon	MR	Mauritania
BF	Burkina Faso	GB	United Kingdom	MW	Malawi
BG	Bulgaria	GN	Guinea	NL	Netherlands
BJ	Benin	GR	Greece	NO	Norway
BR	Brazil	HU	Hungary	PL	Poland
CA	Canada	IT	Italy	RO	Romania
CF	Central African Republic	JP	Japan	SD	Sudan
CG	Congo	KP	Democratic People's Republic of Korea	SE	Sweden
CH	Switzerland	KR	Republic of Korea	SN	Senegal
CI	Côte d'Ivoire	LI	Liechtenstein	SU ⁺	Soviet Union
CM	Cameroon	LK	Sri Lanka	TD	Chad
CS	Czechoslovakia	LU	Luxembourg	TG	Togo
DE ⁺	Germany	MC	Monaco	US	United States of America
DK	Denmark				

⁺ Any designation of "SU" has effect in the Russian Federation. It is not yet known whether any such designation has effect in other States of the former Soviet Union.

METHOD AND APPARATUS FOR PERSONAL IDENTIFICATIONCross Reference to Other Applications

5 This application is a continuation-in-part of
application serial no. 07/341,932 filed April 21,
1989, which is a continuation-in-part of application
serial no. 802,579 filed November 27, 1985, issued
December 5, 1989 as U.S. Patent No. 4,885,778,
which application is itself a continuation-in-part
of application serial no. 676,626 filed November 30,
1984, now U.S. Patent No. 4,720,860, issued January
10 19, 1988. The disclosures and specifications of all
of the foregoing applications/patents are incor-
porated herein by reference as if fully set forth.

- 2 -

Field of the Invention

This invention relates to methods and apparatus for identifying an individual and more particularly to methods and apparatus for providing improved security for a personal identification number (PIN) utilized in conjunction with such an identification system.

Background of the Invention

Personal identification systems may be based on something someone has, such as a card or badge, something that someone knows, such as a PIN, or some characteristic of the individual, such as his fingerprints or speech pattern. Security for such systems is enhanced by utilizing two or more of the above in performing the identification.

For example, parent Patent No. 4,720,860, discloses a personal identification system wherein the individual has a card or other small, portable device which contains a microprocessor programmed to utilize a secret algorithm to generate a nonpredictable number from a stored value unique to the individual and a time varying value provided for example by a clock. The nonpredictable value is preferably displayed on the device. The individual then enters his secret PIN into a central verification system, either directly or over a telephone line, causing the central system to access

- 3 -

stored information corresponding to the individual and to utilize at least some of this information to generate a nonpredictable value at the central computer utilizing the same algorithm as at the individual's microprocessor. At the same time this is being done, the individual is entering the number appearing at that period of time on the display of his device. The two values will match, signifying identification of the individual, only if the individual has entered the correct PIN and if the individual has the proper device so that the nonpredictable code displayed corresponds to that being generated at the central verification computer.

In other systems, such as those shown in U.S. Patent No. 4,599,489 issued July 8, 1986, the PIN may either be stored in the user's device, or may be entered by the user. If the PIN is stored in the device, it is read from the device by a suitable reader and causes the central verification computer to generate a unique challenge code to the individual. This challenge code may either be entered by the individual into his machine, or may be automatically sensed by the machine, and is operated on by the user's device to generate a unique nonpredictable code which is then entered into the central computer to effect verification.

One potential difficulty with either of the systems indicated above is that an unauthorized

- 4 -

individual may be able to obtain access to the user's PIN by electronic eavesdropping, reducing the security provided by the system. If, for example, the PIN is transmitted over public lines, such as telephone lines, from the user to the central verification computer, it may be possible to tap these lines and intercept the PIN as it is being transmitted. If the PIN is stored in the device, someone obtaining the device surreptitiously may, through sophisticated means, be able to determine the PIN stored in the device and thus defeat the security of the system. Furthermore, any storing of a PIN or password in the portable device for comparison defeats the purpose of an independent identification factor and reduces security to a "thing" possessed.

A need therefore exists for an improved means of communicating a PIN or other user identification code to a central verification system such that someone tapping the line over which the code is being sent will be unable to determine the secret identification number and someone obtaining possession of the user device will also not be able to obtain access to the user's secret identification number from the device.

- 5 -

Summary of the Invention

In accordance with the above, this invention provides a method for personal identification and apparatus for the practice thereof wherein a device
5 in the possession of the individual is utilized to generate a unique, time varying, nonpredictable code; the nonpredictable code generated at a given time is mixed with a secret PIN for the individual; the mixed output is communicated to a central
10 verification computer; and the verification computer typically strips the PIN from the communicated value and utilizes the stripped PIN and remaining nonpredictable code to perform a verification operation. Alternatively and equivalently, the
15 mixed output which is communicated to the verification computer may be verified in the verification computer without stripping of the PIN. Preferably, before the mixed value is communicated to the verification computer, a nonsecret
20 identifying code for the individual is communicated to the verification computer; the verification computer utilizes the nonsecret identifying code to obtain the PIN and appropriate nonpredictable code for the individual; and the verification operation
25 includes the PIN and appropriate nonpredictable code obtained during the obtaining step being compared with the stripped PIN and remaining nonpredictable code. Alternatively the PIN may not be stripped

- 6 -

5 from the mixed value, the verification computer may
utilize the nonsecret identifying code to retrieve
or obtain the PIN and appropriate nonpredictable
code, combine the retrieved PIN and appropriate
10 nonpredictable code, and perform a verification
operation between the mixed value communicated to
the verification computer and the combination of the
retrieved PIN and appropriate nonpredictable code.
The verification computer may also generate a unique
15 challenge value in response to the nonsecret
identifying code which challenge code is
communicated to the device in possession of the
individual. For one embodiment, the challenge code
is communicated to the individual and the individual
20 inputs the challenge value and the PIN to his
device, the device includes means responsive to the
challenge value for generating the nonpredictable
code. During the mixing step, the device may
receive the PIN and the nonpredictable code and
25 generate an output which is a predetermined function
of the inputs. The predetermined function may, for
example, be a sum of the inputs, for example the sum
of the inputs without carry.

25 The foregoing and other objects, features and
advantages of the invention will be apparent from
the following more particular description of
preferred embodiments of the invention as
illustrated in the accompanying drawings.

In the Drawings

Fig. 1 is a semi-block schematic diagram of the verification system of a first embodiment of the invention.

5 Fig. 2 is a block schematic diagram of a second embodiment of the invention.

Fig. 3 is a block flow diagram illustrating the operation of the first embodiment of the invention and alternative steps for the second embodiment of the invention.
10

Detailed Description

Fig. 1 shows illustrative structure for a personal identification system of a first embodiment of the invention. In this figure, a user
15 verification device 10 is provided which is of the type described in the parent applications. The device is preferably of the general size and shape of a standard credit card, although its thickness dimension may be slightly greater than that of such
20 cards. The device 10 has a clock which generates a time-dependent digital output to a microprocessor which is programmed with a unique algorithm to operate on the time-dependent clock input and on a stored static value unique to a given user to
25 generate a multi-bit nonpredictable code. A plurality of input areas 12 are provided on the face of device 10. These areas are preferably each

- 8 -

indicative of a numerical digit, for example the digits 1 - 0 as shown in Fig. 1, and may be pressure-sensitive pads or otherwise adapted to generate an electrical output indicative of the area when the area is touched by the user. Spacing may be provided between the individual areas 12 to assure distinctive outputs. As will be described in greater detail hereinafter, the user may input his unique PIN on areas 12 which are mixed in the processor in device 10 with the nonpredictable code generated therein in response to the time-dependent and static inputs to generate a multi-bit nonpredictable code which is displayed on area 14 of device 10. Area 14 may be a liquid crystal display or other suitable display device for producing numeric or alpha-numeric characters. Each area of display 14 is adapted to display a different digit of the nonpredictable code.

The user initially transmits a nonsecret identifying code to verification computer 16 by keying this number into a telephone 18 at his location. This number is transmitted over telephone lines 20 to telephone 22 at the verification station and through a modem 24 at this station to the verification computer. The user may then use the telephone 18 to key in and transmit the nonpredictable code being displayed at that time on display 14.

- 9 -

Fig. 3 is a flow diagram illustrating in greater detail the operation of the system of Fig. 1 to perform a verification operation. Referring to Fig. 3, the first step in the operation, step 30, is for the user to send his nonsecret code to verification computer (VC) 16. As previously indicated, this is accomplished by the user keying his nonsecret identification number into telephone 18 for transmission through telephone line 20, telephone 22 and modem 24 to the verification computer.

In response to the user input of his nonsecret code, the verification computer retrieves the user's PIN and generates the nonpredictable code for the user, using the same algorithm and stored static value as user device 10, and using a time-related value from a clock device at the verification computer, which is maintained in synchronism with the clock at the user device in a manner discussed in the parent application (step 32). At the same time that the verification computer is retrieving the PIN and nonpredictable code for the user, the user is inputting his PIN into his device 10 using key pads or areas 12 (step 34). While the user is inputting his pin, the user device is continuously generating nonpredictable code values at its internal processor in response to the clock value and the stored static value using the unique algorithm at the user device processor (step 36).

- 10 -

The next step in the operation, step 38, is for the generated nonpredictable code and the inputted pin to be mixed by the processor in device 10 to generate a new nonpredictable code which is
5 displayed on display 14. The mixing operation may be a simple addition of the two values without carry, or with carry, (a constant added to a pseudo random number produces a pseudo random number) or may involve a more sophisticated mixing algorithm.

10 During step 40, the user transmits the displayed value by use of telephone 18 through telephone line 20, telephone 22, and modem 24 to verification computer 16.

15 During the next step in the operation, step 42, the verification computer uses the PIN for the user which was retrieved during step 32 to strip the PIN from the inputted nonpredictable code, the result being a PIN value and a nonpredictable code value. During step 44 the stripped PIN is compared with the
20 PIN retrieved during step 32 and during step 46 the nonpredictable code remaining after the inputted value has the PIN stripped therefrom is compared with the retrieved nonpredictable code. If matches are obtained during both steps 44 and 46 (step 48)
25 the verification computer signifies verification. If a match is not found during either step 44 or step 46 (step 50) then the user is rejected.

- 11 -

Alternatively to steps 42, 44, 46, 48 and 50, the PIN and nonpredictable code which are retrieved in step 32 may be combined or mixed by the verification computer during step 142 according to the same mixing operation which was carried out by the processor or user device 10 in step 38, e.g. by a simple addition of the two values without carry, with carry, or according to some other more sophisticated algorithm. During alternative step 144 the separate results of the mixing operations carried out by the user device 10 and the verification computer 16 are compared. If a match is obtained, step 148, the user is verified. If a match is not found, step 150, the user is rejected.

A procedure is thus provided wherein user verification may be obtained using the simple and inexpensive procedure disclosed in the parent applications while still providing a high level of security for the user PIN. This security is achieved since the user PIN is never available on an open line which could be tapped except in the form of a word which is a mixture of the PIN with a nonpredictable code and which is virtually impossible to decipher.

Fig. 2 illustrates an alternative configuration in which the teachings of this invention may be utilized. In Fig. 2, the user device 10 is of the same type shown in Fig. 1. However, for this

- 12 -

embodiment of the invention, the user device is adapted to be used in proximity to the verification station rather than from a remote location over telephone lines. For this embodiment of the invention, the verification station 60 includes a computer 62, a display 64, such as for example a CRT display, and an input device 66 which may, for example, be a standard computer input keyboard. Referring again to Fig. 3, the operation with this embodiment of the invention starts with step 30, during which the user sends a nonsecret code to the verification computer 62 by, for example, keying this code into input device 66. In response to receiving the nonsecret code, computer 60 retrieves the PIN and generates the nonpredictable code for the user (step 32) and also retrieves a challenge code for the user which is displayed on display 64 (step 70). The user inputs his PIN and the challenge code in an order established for the system to user device 10 using input pads 12 (step 72). During step 74, the processor in device 10 uses the inputted challenge code and the time inputted from its clock to generate a nonpredictable code which, during step 38, is mixed with the inputted pin and the results are displayed on display 14 of device 10. From this point on, the operation for this embodiment of the invention is the same as that previously described with respect to the embodiment of Fig. 1.

- 13 -

Thus, with this embodiment of the invention, as with the prior embodiment of the invention, the pin in uncoded form is never transmitted in a manner such that it could be observed and is not resident in the user's device where it might, using
5 sophisticated technology, be retrieved.

As an alternative to the embodiment shown in Fig. 2, the nonsecret code may be recorded in machine-readable form on device 10 and input device
10 66 might include a card reader which the card is inserted into to permit the nonsecret code to be read into computer 62.

While the invention has been shown and described above with reference to preferred embodiments, the
15 foregoing and other changes in form and detail may be made therein by one skilled in the art without departing from the spirit and scope of the invention.

What is claimed is:

- 14 -

CLAIMS

1. In a personal identification system of the type wherein a user is provided with a device generating a unique, time-varying, nonpredictable code, with a nonsecret identifying code and with a secret PIN, the nonpredictable code at a given instant and the PIN being provided to a central verification computer to effect verification; apparatus for providing improved security for the PIN comprising:

means for mixing the nonpredictable code generated by the device at a given time with the PIN according to a predetermined algorithm to generate a combined coded value;

means for separately communicating the nonsecret identifying code and the combined coded value to the central verification computer; and

wherein the central verification computer includes means for utilizing the nonsecret identifying code to retrieve the PIN and generate an appropriate, unique, time varying nonpredictable code for the individual, and at least one of:

(a) a means for utilizing the retrieved PIN, appropriate nonpredictable code and the combined coded value in performing a verification operation; or

- 15 -

(b) a means for stripping the PIN from the combined coded value received from the means for communicating, the nonpredictable code remaining after stripping of the PIN and means for utilizing the retrieved PIN, and appropriate nonpredictable code for performing a verification operation.

2. Apparatus as claimed in claim 1 including means operative prior to the communicating of the value from the mixing means for communicating the nonsecret identifying code to said verification computer.

3. Apparatus as claimed in claim 2 wherein said verification computer includes means for utilizing the communicated nonsecret identifying code to retrieve the PIN and a unique challenge value for the individual; and means for communicating the challenge value to the device.

4. Apparatus as claimed in claim 3 wherein said challenge value communicating means includes means for communicating the challenge value to the individual; and wherein the device includes means for permitting the individual to input the challenge value and his PIN to the device.

- 16 -

5. Apparatus as claimed in claim 4 wherein said device includes means responsive to the challenge value for generating the nonpredictable code; and

5 wherein said mixing means includes means, included as part of the device, for receiving the inputted PIN and the generated nonpredictable value and for generating an output which is a predetermined function of the input.

10 6. Apparatus as claimed in claim 5 wherein said mixing means adds the PIN to the nonpredictable code.

7. Apparatus as claimed in claim 1 wherein said device includes means for permitting the individual to input his PIN to the device; and

15 wherein said means for mixing is included as part of said device and is adapted to receive the PIN inputted by the individual and the nonpredictable code and to generate an output which

20 is a predetermined function of the input.

8. Apparatus as claimed in claim 7 wherein said mixing means adds the PIN to the nonpredictable code.

- 17 -

5 9. Apparatus as claimed in claim 1 wherein said verification computer includes a means for mixing the retrieved PIN and appropriate nonpredictable code generated by the verification computer at a given time according to the predetermined algorithm to generate a second combined coded value.

10 10. Apparatus as claimed in claim 9 wherein the verification operation comprises comparing the combined coded value with the second combined coded value.

15 11. Apparatus as claimed in claim 1 wherein the means for performing a verification operation includes means for comparing the PIN and nonpredictable code obtained in response to the nonsecret identifying code with the stripped PIN and remaining nonpredictable code.

20 12. A method for identifying an individual comprising the steps of:
utilizing a device in the possession of the individual to generate a unique time-varying, nonpredictable code;
25 mixing the nonpredictable code generated at a given time with a secret PIN for the individual to generate a combined code; and

- 18 -

communicating a nonsecret identifying code for the individual and the combined code to a central verification computer;

5 the verification computer utilizing the nonsecret identifying code to retrieve the PIN and generate an appropriate, unique, time-varying nonpredictable code for the individual, and at least one of:

10 (a) utilizing the retrieved PIN, appropriate nonpredictable code, and the combined code to perform a verification operation; or
(b) stripping the PIN from the communicated combined code and utilizing the retrieved PIN and nonpredictable code, the stripped
15 PIN and the remaining nonpredictable code to perform a verification operation.

13. A method as claimed in claim 12 wherein the verification
20 computer also generates a unique challenge value in response to the nonsecret identifying code; and including the step of communicating the challenge value to the device in possession of the individual.

14. A method as claimed in claim 13 wherein the
25 challenge value is communicated to the individual; and

- 19 -

including the step of the individual inputting the challenge value and his PIN to the device.

5 15. A method as claimed in claim 14 wherein the device includes means responsive to the challenge value for generating the nonpredictable code; and
 wherein the mixing step includes the device receiving the PIN and the nonpredictable code and generating an output which is a predetermined
10 function of the inputs.

 16. A method as claimed in claim 15 wherein said predetermined function is a sum of said inputs.

15 17. A method as claimed in claim 15 including the step of the individual inputting his PIN to the device; and

 wherein the mixing step includes the device receiving the PIN inputted by the individual and the nonpredictable code and generating an output which is a predetermined function of the inputs.

20 18. A method as claimed in claim 17 wherein said predetermined function is a sum of said input.

 19. A method as claimed in claim 12 wherein the verification computer utilizes the retrieved PIN and

- 20 -

appropriate nonpredictable code by combining them to obtain a second combined code.

20. A method as claimed in claim 19 wherein the verification operation comprises comparing the
5 combined code and the second combined code.

21. A method as claimed in claim 12 wherein the verification operation includes comparing the
retrieved PIN and the nonpredictable code generated
by the verification computer with the stripped PIN
10 and the remaining nonpredictable code.

1/2

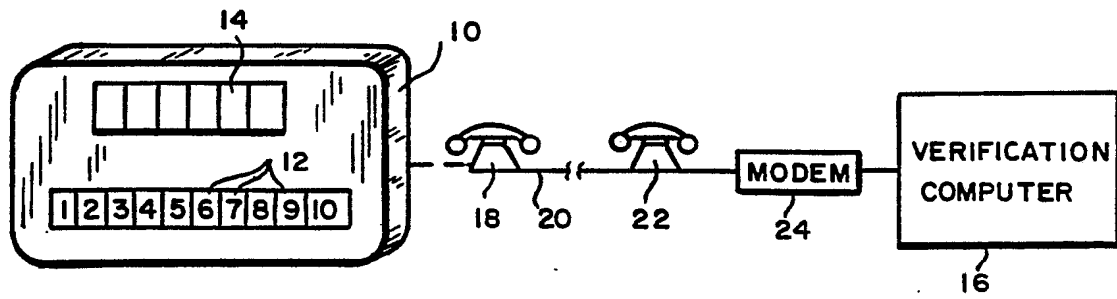


FIG. 1

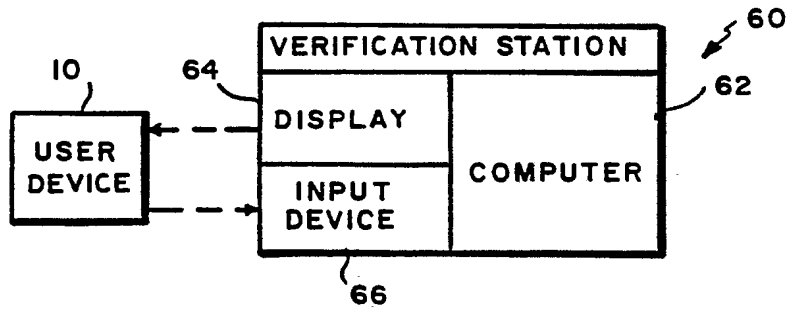


FIG. 2

2/2

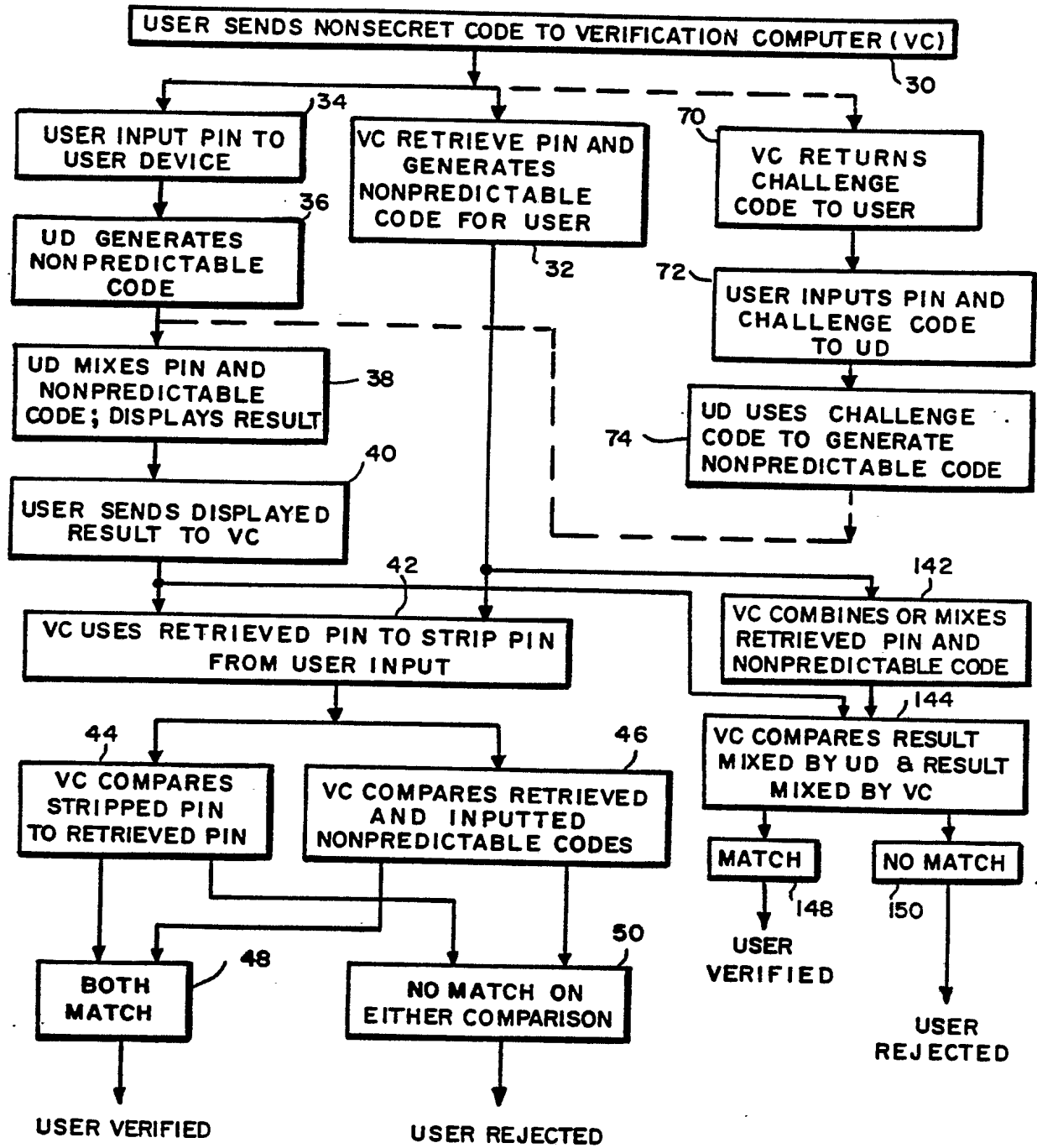


FIG.3

INTERNATIONAL SEARCH REPORT

International Application No. PCT/US91/03034

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) ⁶		
According to International Patent Classification (IPC) or to both National Classification and IPC		
IPC(5) H04K 1/00 US 380/23,25		
II. FIELDS SEARCHED		
Minimum Documentation Searched ⁷		
Classification System	Classification Symbols	
US	380/23,24,25,28,48	
Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched ⁸		
III. DOCUMENTS CONSIDERED TO BE RELEVANT ⁹		
Category ⁹	Citation of Document, ¹¹ with indication, where appropriate, of the relevant passages ¹²	Relevant to Claim No. ¹³
X	US,A 4,720,860 (WEISS) 19 January 1988	1-21
A	US,A 4,890,323 (BEKER ET AL) 26 December 1989	1-21
A	US,A 4,885,778 (WEISS) 05 December 1989	1-21
A	US,A 4,856,062 (WEISS) 08 August 1989	1-21
A	US,A 4,819,267 (CARGILE ET AL) 04 April 1989	1-21
A	US,A 4,802,216 (IRWIN ET AL) 31 January 1989	1-21
A	US,A 4,731,841 (ROSEN ET AL) 15 March 1988	1-21
A	US,A 4,599,489 (CARGILE) 08 July 1986	1-21
A	US,A 4,578,530 (ZEIDLER) 25 March 1986	1-21
A	US,A 4,509,093 (STELLBERGER) 02 April 1985	1-21
<p>¹⁰ Special categories of cited documents:</p> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier document but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p> <p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.</p> <p>"&" document member of the same patent family</p>		
IV. CERTIFICATION		
Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report	
21 August 1991	27 SEP 1991	
International Searching Authority	Signature of Authorized Officer <i>Ngoc Ho Nguyen</i>	
ISA/US	David Cain NGUYEN NGOC-HO INTERNATIONAL DIVISION	

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

PCT

NOTIFICATION OF TRANSMITTAL OF
THE INTERNATIONAL SEARCH REPORT AND
THE WRITTEN OPINION OF THE INTERNATIONAL
SEARCHING AUTHORITY, OR THE DECLARATION

To:

LOWRIE, LANDO & ANASTASI, LLP
Attn. Anastasi, John N.
One Main Street Suite 1100
Cambridge, MA 02142
ETATS-UNIS D'AMERIQUE

(PCT Rule 44.1)

Date of mailing (day/month/year) 11/03/2008	
Applicant's or agent's file reference W0537-7010W0	FOR FURTHER ACTION See paragraphs 1 and 4 below
International application No. PCT/US2007/070701	International filing date (day/month/year) 08/06/2007
Applicant WEISS, Kenneth P.	COPY

1. The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

Filing of amendments and statement under Article 19:

The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

When? The time limit for filing such amendments is normally two months from the date of transmittal of the International Search Report.

Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes
1211 Geneva 20, Switzerland, Facsimile No.: (41-22) 338.82.70

For more detailed instructions, see the notes on the accompanying sheet.

2. The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

- the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.
 no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. Reminders


Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90*bis*.1 and 90*bis*.3, respectively, before the completion of the technical preparations for international publication.

The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the International Searching Authority  European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Pilvi Koski
--	-----------------------------------

NOTES TO FORM PCT/ISA/220

These Notes are intended to give the basic instructions concerning the filing of amendments under article 19. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the *PCT Applicant's Guide*, a publication of WIPO.

In these Notes, "Article", "Rule", and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions, respectively.

INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report and the written opinion of the International Searching Authority, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims, description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the latter to be published for the purposes of provisional protection or has another reason for amending the claims before international publication. Furthermore, it should be emphasized that provisional protection is available in some States only (see *PCT Applicant's Guide*, Volume I/A, Annexes B1 and B2).

The attention of the applicant is drawn to the fact that amendments to the claims under Article 19 are not allowed where the International Searching Authority has declared, under Article 17(2), that no international search report would be established (see *PCT Applicant's Guide*, Volume I/A, paragraph 296).

What parts of the international application may be amended?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

When?

Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the International Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 46.1).

Where not to file the amendments?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 46.2).

Where a demand for international preliminary examination has been/is filed, see below.

How?

Either by cancelling one or more entire claims, by adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet must be submitted for each sheet of the claims which, on account of an amendment or amendments, differs from the sheet originally filed.

All the claims appearing on a replacement sheet must be numbered in Arabic numerals. Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively (Section 205(b)).

The amendments must be made in the language in which the international application is to be published.

What documents must/may accompany the amendments?

Letter (Section 205(b)):

The amendments must be submitted with a letter.

The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 19(1)" (see below, under "Statement under Article 19(1)").

The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference W0537-7010WO	FOR FURTHER ACTION		see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US2007/070701	International filing date (day/month/year) 08/06/2007	(Earliest) Priority Date (day/month/year) 09/06/2006	
Applicant WEISS, Kenneth P.			

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 4 sheets.

It is also accompanied by a copy of each prior art document cited in this report.

1. Basis of the report

a. With regard to the **language**, the international search was carried out on the basis of:

- the International application in the language in which it was filed
- a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))

b. This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6bis(a)).

c. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. **Certain claims were found unsearchable** (See Box No. II)

3. **Unity of invention is lacking** (see Box No III)

4. With regard to the **title**,

- the text is approved as submitted by the applicant
- the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

- the text is approved as submitted by the applicant
- the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings**,

a. the figure of the **drawings** to be published with the abstract is Figure No. 21

- as suggested by the applicant
- as selected by this Authority, because the applicant failed to suggest a figure
- as selected by this Authority, because this figure better characterizes the invention

b. none of the figures is to be published with the abstract

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06F21/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004/034771 A1 (EDGETT JEFF STEVEN [US] ET AL) 19 February 2004 (2004-02-19) figure 3 paragraph [0048] - paragraph [0050]	1,27-32, 38-40
X	US 2001/044900 A1 (UCHIDA KAORU [JP]) 22 November 2001 (2001-11-22) paragraph [0039]; figure 4	2-10,41, 42,67-75
X	US 2005/039027 A1 (SHAPIRO MICHAEL F [US]) 17 February 2005 (2005-02-17) abstract figure 2 paragraph [0015] - paragraph [0017] paragraph [0021] - paragraph [0022] paragraph [0024]	41-44
	----- -/--	

 Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *Z* document member of the same patent family

Date of the actual completion of the international search

26 February 2008

Date of mailing of the international search report

11/03/2008

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Chabot, Pedro

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT.

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 986 209 A (MITSUBISHI ELECTRIC CORP [JP]) 15 March 2000 (2000-03-15) paragraph [0012] - paragraph [0013] -----	1-75

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2007/070701

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 2004034771	A1	19-02-2004	NONE	
US 2001044900	A1	22-11-2001	JP 2001325549 A	22-11-2001
US 2005039027	A1	17-02-2005	NONE	
EP 0986209	A	15-03-2000	AU 718480 B2	13-04-2000
			AU 3912199 A	16-03-2000
			CN 1248114 A	22-03-2000
			DE 69929267 T2	31-08-2006
			HK 1026542 A1	05-08-2005
			JP 2000092046 A	31-03-2000
			US 6751733 B1	15-06-2004

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

PCT

To:

see form PCT/ISA/220

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY
(PCT Rule 43bis.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference see form PCT/ISA/220	FOR FURTHER ACTION See paragraph 2 below
---	--

International application No. PCTUS2007/070701	International filing date (day/month/year) 08.06.2007	Priority date (day/month/year) 09.06.2006
---	--	--

International Patent Classification (IPC) or both national classification and IPC
INV. G06F21/00

Applicant
WEISS, Kenneth P.

1. This opinion contains indications relating to the following items:

- Box No. I Basis of the opinion
- Box No. II Priority
- Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- Box No. IV Lack of unity of invention
- Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- Box No. VI Certain documents cited
- Box No. VII Certain defects in the international application
- Box No. VIII Certain observations on the international application


2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA:  European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465	Date of completion of this opinion see form PCT/ISA/210	Authorized Officer Chabot, Pedro Telephone No. +49 89 2399-6085
---	--	---



Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:
 - the international application in the language in which it was filed
 - a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).
2. This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))
3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:
 - a. type of material:
 - a sequence listing
 - table(s) related to the sequence listing
 - b. format of material:
 - on paper
 - in electronic form
 - c. time of filing/furnishing:
 - contained in the international application as filed.
 - filed together with the international application in electronic form.
 - furnished subsequently to this Authority for the purposes of search.
4. In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
5. Additional comments:

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes: Claims	<u>11-26,33-37,45-66</u>
	No: Claims	<u>1-10,27-32,38-44,67-75</u>
Inventive step (IS)	Yes: Claims	
	No: Claims	<u>1-75</u>
Industrial applicability (IA)	Yes: Claims	<u>1-75</u>
	No: Claims	

2. Citations and explanations

see separate sheet

Re Item V.

1 Reference is made to the following documents:

- D1 : US 2004/034771 A1 (EDGETT JEFF STEVEN [US] ET AL) 19 February 2004 (2004-02-19)
- D2 : EP 0 986 209 A (MITSUBISHI ELECTRIC CORP [JP]) 15 March 2000 (2000-03-15)
- D3 : US 2001/044900 A1 (UCHIDA KAORU [JP]) 22 November 2001 (2001-11-22)
- D4 : US 2005/039027 A1 (SHAPIRO MICHAEL F [US]) 17 February 2005 (2005-02-17)

2 The present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of claim 1 is not new in the sense of Article 33(2) PCT.

Document D1 discloses (the references in parentheses applying to this document):

- a) A method of authenticating an identity of a first entity (Par. 48-50).
- b) Wirelessly transmitting from a first device, first encrypted authentication information of the first entity (par. 49 lines 3-8, It is considered that the network includes wireless means that are being used in the transmission).
- c) Receiving with a second device the wirelessly transmitted first encrypted authentication information (par. 49 line 8).
- d) Decrypting with the second device, the first wirelessly encrypted authentication information to provide the first authentication information of the first entity to the second device (par. 49 lines 20-24).
- e) Authenticating the identity of the first entity based upon the first authentication information and acting based on the authenticated identity of the first entity (par. 50).

3 The present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of claim 41 is not new in the sense of Article 33(2) PCT.

Document D4 discloses (the references in parentheses applying to this document):

- a) A system for validating an identity of a first entity comprising a first wireless device comprising (par. 5).
 - b) A first wireless transmitter and receiver configured to transmit a first wireless signal including first encrypted authentication information (par. 5 l.33-36).
 - c) A first processor configured to compare stored biometric data with detected biometric data of the first entity and configured to enable or disable use of the first device based on a result of the comparison, and configured to encrypt first authentication information with a first private key into the first encrypted authentication information (par. 5 l.19-21, par. 15 l.34-36, par. 16 l.7-10 and par. 17).
 - d) A first biometric detector for detecting biometric data of the first entity (par. 5 l.21-25).
 - e) A first memory for storing biometric data of the first entity, a private key of the first entity authorized to use the first device, and the first authentication information (par. 5 l.19-21).
- 4 The present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of claim 67 is not new in the sense of Article 33(2) PCT.
Document D3 discloses (the references in parentheses applying to this document):
- a) A first wireless device (par. 30 and par. 54).
 - b) A processor configured to enable operation of the first wireless device if it receives an enablement signal validating first biometric information of a first entity and configured to generate a non-predictable signal from the biometric information (par. 36 The processor generates a non-predictable signal from the biometric data when it encrypts the data.)
 - c) A first wireless transmitter and receiver configured to transmit a first wireless signal including first encrypted biometric information of the first entity and to receive the enablement signal (par. 30, 36 and 39 The enablement signal comes from the authentication server via the ECSP unit in the form of a service).
 - d) A first biometric detector for detecting the first biometric information of the first entity (par. 36).
- 5 Dependent claims 2-40, 42-66, 68-75 do not contain any features which, in

combination with the features of any claim to which they refer, meet the requirements of the PCT in respect of novelty and/or inventive step (Article 33(2) and (3) PCT).

The dependent claims contain features that are part of the common general knowledge like encryption methods, biometric data capture devices and methods for securing communications. These features represent mere implementation details that are well-known to the person skilled in the art, and will not justify an inventive activity.

It is worth to say that the application merely contains a juxtaposition of different techniques used in authentication and cryptography functioning in their normal way and not producing any non-obvious working inter-relationship that justifies an inventive activity.

Possible steps after receipt of the international search report (ISR) and written opinion of the International Searching Authority (WO-ISA)

General information

For all international applications filed on or after 01/01/2004 the competent ISA will establish an ISR. It is accompanied by the WO-ISA. Unlike the former written opinion of the IPEA (Rule 66.2 PCT), the WO-ISA is not meant to be responded to, but to be taken into consideration for further procedural steps. This document explains about the possibilities.

Amending claims under Art. 19 PCT

Within 2 months after the date of mailing of the ISR and the WO-ISA the applicant may file amended claims under Art. 19 PCT directly with the International Bureau of WIPO. The PCT reform of 2004 did not change this procedure. For further information please see Rule 46 PCT as well as form PCT/ISA/220 and the corresponding Notes to form PCT/ISA/220.

Filing a demand for international preliminary examination

In principle, the WO-ISA will be considered as the written opinion of the IPEA. This should, in many cases, make it unnecessary to file a demand for international preliminary examination. If the applicant nevertheless wishes to file a demand this must be done before expiry of 3 months after the date of mailing of the ISR/ WO-ISA or 22 months after priority date, whichever expires later (Rule 54bis PCT). Amendments under Art. 34 PCT can be filed with the IPEA as before, normally at the same time as filing the demand (Rule 66.1 (b) PCT).

If a demand for international preliminary examination is filed and no comments/amendments have been received the WO-ISA will be transformed by the IPEA into an IPRP (International Preliminary Report on Patentability) which would merely reflect the content of the WO-ISA. The demand can still be withdrawn (Art. 37 PCT).

Filing informal comments

After receipt of the ISR/WO-ISA the applicant may file informal comments on the WO-ISA directly with the International Bureau of WIPO. These will be communicated to the designated Offices together with the IPRP (International Preliminary Report on Patentability) at 30 months from the priority date. Please also refer to the next box.

End of the international phase

At the end of the international phase the International Bureau of WIPO will transform the WO-ISA or, if a demand was filed, the written opinion of the IPEA into the IPRP, which will then be transmitted together with possible informal comments to the designated Offices. The IPRP replaces the former IPER (international preliminary examination report).

Relevant PCT Rules and more information

Rule 43 PCT, Rule 43bis PCT, Rule 44 PCT, Rule 44bis PCT, PCT Newsletter 12/2003, OJ 11/2003, OJ 12/2003

PATENT COOPERATION TREATY

W0537-700910

From the INTERNATIONAL SEARCHING AUTHORITY

PCT

To:

LOWRIE, LANDO & ANASTASI, LLP
 Attn. Donahoe, Robert V.
 One Main Street Suite 1100
 Cambridge, MA 02142
 ETATS-UNIS D'AMERIQUE

Reviewed by
 Docketing
 12/11/07

NOTIFICATION OF TRANSMITTAL OF
 THE INTERNATIONAL SEARCH REPORT AND
 THE WRITTEN OPINION OF THE INTERNATIONAL
 SEARCHING AUTHORITY, OR THE DECLARATION

(PCT Rule 44.1)

Date of mailing (day/month/year)	27/11/2007
Applicant's or agent's file reference W0537-7009W0	FOR FURTHER ACTION See paragraphs 1 and 4 below
International application No. PCT/US2007/004646	International filing date (day/month/year) 21/02/2007
Applicant WEISS, Kenneth P.	DOCKETED <i>Amend Claims on formal 1.27.08</i> DUE: <i>resp to WOI 2.27.08</i>

1. The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

Filing of amendments and statement under Article 19:

The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

When? The time limit for filing such amendments is normally two months from the date of transmittal of the International Search Report.

Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes
 1211 Geneva 20, Switzerland, Facsimile No.: (41-22) 338.82.70

For more detailed instructions, see the notes on the accompanying sheet.

2. The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

- the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.
 no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**


Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90bis.1 and 90bis.3, respectively, before the completion of the technical preparations for international publication.

The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the International Searching Authority  European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Katrin Sommermeyer
---	--

NOTES TO FORM PCT/ISA/220

These Notes are intended to give the basic instructions concerning the filing of amendments under article 19. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the *PCT Applicant's Guide*, a publication of WIPO.

In these Notes, "Article", "Rule", and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions, respectively.

INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report and the written opinion of the International Searching Authority, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims, description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the latter to be published for the purposes of provisional protection or has another reason for amending the claims before international publication. Furthermore, it should be emphasized that provisional protection is available in some States only (see *PCT Applicant's Guide*, Volume I/A, Annexes B1 and B2).

The attention of the applicant is drawn to the fact that amendments to the claims under Article 19 are not allowed where the International Searching Authority has declared, under Article 17(2), that no international search report would be established (see *PCT Applicant's Guide*, Volume I/A, paragraph 296).

What parts of the international application may be amended?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

When?

Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the international Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 46.1).

Where not to file the amendments?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 46.2).

Where a demand for international preliminary examination has been/is filed, see below.

How?

Either by cancelling one or more entire claims, by adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet must be submitted for each sheet of the claims which, on account of an amendment or amendments, differs from the sheet originally filed.

All the claims appearing on a replacement sheet must be numbered in Arabic numerals. Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively (Section 205(b)).

The amendments must be made in the language in which the international application is to be published.

What documents must/may accompany the amendments?

Letter (Section 205(b)):

The amendments must be submitted with a letter.

The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 19(1)" (see below, under "Statement under Article 19(1)").

The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference W0537-7009WO	FOR FURTHER ACTION		see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US2007/004646	International filing date (day/month/year) 21/02/2007	(Earliest) Priority Date (day/month/year) 21/02/2006	
Applicant WEISS, Kenneth P.			

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 6 sheets.

It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**

a. With regard to the **language**, the international search was carried out on the basis of:

- the international application in the language in which it was filed
- a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))

b. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. **Certain claims were found unsearchable** (See Box No. II)

3. **Unity of invention is lacking** (see Box No III)

4. With regard to the **title**,

- the text is approved as submitted by the applicant
- the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

- the text is approved as submitted by the applicant
- the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings**,

- a. the figure of the **drawings** to be published with the abstract is Figure No. 1
 - as suggested by the applicant
 - as selected by this Authority, because the applicant failed to suggest a figure
 - as selected by this Authority, because this figure better characterizes the invention
- b. none of the figures is to be published with the abstract

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2007/004646

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06F21/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GB 2 382 006 A (IBM [US]) 14 May 2003 (2003-05-14) figure 3 page 4, line 29 - line 34 page 17, line 10 - line 27 page 18, line 5 - line 24	1,63
Y	----- US 2005/001711 A1 (DOUGHTY RALPH O [US] ET AL) 6 January 2005 (2005-01-06) paragraph [0012] paragraph [0061] -----	2-9,13, 20-22, 64-84
Y	US 2005/001711 A1 (DOUGHTY RALPH O [US] ET AL) 6 January 2005 (2005-01-06) paragraph [0012] paragraph [0061]	2-9,13, 20-22, 64-84

Further documents are listed in the continuation of Box C.

See patent family annex.

- * Special categories of cited documents :
- *A* document defining the general state of the art which is not considered to be of particular relevance
 - *E* earlier document but published on or after the international filing date
 - *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
 - *O* document referring to an oral disclosure, use, exhibition or other means
 - *P* document published prior to the international filing date but later than the priority date claimed
 - *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
 - *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
 - *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
 - * & * document member of the same patent family

Date of the actual completion of the international search 13 November 2007	Date of mailing of the international search report 27/11/2007
---	--

Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Chabot, Pedro
---	---

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US2007/004646

Box II Observations where certain claims were found unsearchable (Continuation of item 2 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box III Observations where unity of invention is lacking (Continuation of item 3 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

1-9, 13-14, 20-22, 63-84

4. No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

- The additional search fees were accompanied by the applicant's protest.
- No protest accompanied the payment of additional search fees.

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1,63

Giving authorization for an operation to a second device by a third device depending on information given by a first device.

2. claims: 2-9, 20-22, 13-14,64-84

Emulating a credit card and providing the services associated to the credit card.

3. claims: 10-12, 38-41,46,47, 100-103, 108-109

Secure communications between the first and the second devices using cryptography.

4. claims: 15-19, 24-32, 86-94

Different methods of authenticating the user at a second the device, using user information sent from the first device.

5. claims: 33-37, 95-99

Accessing user information from a data base by the secure system. The secure system access user authentication information and send it to the second device.

6. claims: 42-45, 48-62, 104-107, 110-124

Authentication of a user at a first device, a second user at a second device, sending authentication information from the first device to the second to authenticate the first user at the second device. Permit two users to manipulate their respective devices and authenticate the one first user by the second via information sent from the first device to the second.

7. claims: 23,85 125, 129

Send to credit card information for validation at a credit card service.

8. claims: 126-128, 130-132

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

Information validation based on information sent from a
first and third devices to a second device.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2007/004646

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2382006	A	14-05-2003	NONE
US 2005001711	A1	06-01-2005	NONE

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

PCT

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY
(PCT Rule 43bis.1)

To:

see form PCT/ISA/220

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference
see form PCT/ISA/220

FOR FURTHER ACTION
See paragraph 2 below

International application No.
PCT/US2007/004646

International filing date (day/month/year)
21.02.2007

Priority date (day/month/year)
21.02.2006

International Patent Classification (IPC) or both national classification and IPC
INV. G06F21/00

Applicant
WEISS, Kenneth P.

1. This opinion contains indications relating to the following items:

- Box No. I Basis of the opinion
- Box No. II Priority
- Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- Box No. IV Lack of unity of invention
- Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- Box No. VI Certain documents cited
- Box No. VII Certain defects in the international application
- Box No. VIII Certain observations on the international application

2. **FURTHER ACTION**


If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

Name and mailing address of the ISA:



European Patent Office
D-80298 Munich
Tel. +49 89 2399 - 0 Tx: 523656 epmu d
Fax: +49 89 2399 - 4465


Date of completion of this opinion

see form PCT/ISA/210

Authorized Officer

Chabot, Pedro

Telephone No. +49 89 2399-6085



Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:
 - the international application in the language in which it was filed
 - a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).
2. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:
 - a. type of material:
 - a sequence listing
 - table(s) related to the sequence listing
 - b. format of material:
 - on paper
 - in electronic form
 - c. time of filing/furnishing:
 - contained in the international application as filed.
 - filed together with the international application in electronic form.
 - furnished subsequently to this Authority for the purposes of search.
3. In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
4. Additional comments:

Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability

The questions whether the claimed invention appears to be novel, to involve an inventive step (to be non obvious), or to be industrially applicable have not been examined in respect of

- the entire international application
- claims Nos. 10-12,15-19,23-62, 85-132

because:

- the said international application, or the said claims Nos. relate to the following subject matter which does not require an international search (*specify*):
- the description, claims or drawings (*indicate particular elements below*) or said claims Nos. are so unclear that no meaningful opinion could be formed (*specify*):
- the claims, or said claims Nos. are so inadequately supported by the description that no meaningful opinion could be formed (*specify*):
- no international search report has been established for the whole application or for said claims Nos. 10-12,15-19,23-62, 85-132
- a meaningful opinion could not be formed without the sequence listing; the applicant did not, within the prescribed time limit:
 - furnish a sequence listing on paper complying with the standard provided for in Annex C of the Administrative Instructions, and such listing was not available to the International Searching Authority in a form and manner acceptable to it.
 - furnish a sequence listing in electronic form complying with the standard provided for in Annex C of the Administrative Instructions, and such listing was not available to the International Searching Authority in a form and manner acceptable to it.
 - pay the required late furnishing fee for the furnishing of a sequence listing in response to an invitation under Rules 13^{ter}.1(a) or (b).
- a meaningful opinion could not be formed without the tables related to the sequence listings; the applicant did not, within the prescribed time limit, furnish such tables in electronic form complying with the technical requirements provided for in Annex C-bis of the Administrative Instructions, and such tables were not available to the International Searching Authority in a form and manner acceptable to it.
- the tables related to the nucleotide and/or amino acid sequence listing, if in electronic form only, do not comply with the technical requirements provided for in Annex C-bis of the Administrative Instructions.
- See Supplemental Box for further details

Box No. IV Lack of unity of invention

1. In response to the invitation (Form PCT/ISA/206) to pay additional fees, the applicant has, within the applicable time limit:
- paid additional fees
 - paid additional fees under protest and, where applicable, the protest fee
 - paid additional fees under protest but the applicable protest fee was not paid
 - not paid additional fees
2. This Authority found that the requirement of unity of invention is not complied with and chose not to invite the applicant to pay additional fees.
3. This Authority considers that the requirement of unity of invention in accordance with Rule 13.1, 13.2 and 13.3 is
- complied with
 - not complied with for the following reasons:
see separate sheet
4. Consequently, this report has been established in respect of the following parts of the international application:
- all parts.
 - the parts relating to claims Nos. 1-9,13-14,20-22,63-84

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes: Claims	<u>2-9,13-14,20-22,64-84</u>
	No: Claims	<u>1,63</u>
Inventive step (IS)	Yes: Claims	
	No: Claims	<u>1-9,13-14,20-22,63-84</u>
Industrial applicability (IA)	Yes: Claims	<u>1-9,13-14,20-22,63-84</u>
	No: Claims	

2. Citations and explanations

see separate sheet

Re Item III.

No opinion is given for claims 10-12,15-19,23-62 and 85-132 as no search report has been established for those claims.

Re Item IV.

The separate inventions/groups of inventions are:

I Claims 1,63:

Giving authorization for an operation to a second device by a third device depending on information given by a first device.

II Claims 2-9, 20-22, 13-14,64-84:

Emulating a credit card and providing the services associated to the credit card.

III Claims 10-12, 38-41,46,47, 100-103, 108-109:

Secure communications between the first and the second devices using cryptography.

IV Claims 15-19, 24-32, 86-94:

Different methods of authenticating the user at a second the device, using user information sent from the first device.

V Claims 33-37, 95-99:

Accessing user information from a data base by the secure system. The secure system access user authentication information and send it to the second device.

VI Claims 42-45, 48-62, 104-107, 110-124:

Authentication of a user at a first device, a second user at a second device, sending authentication information from the first device to the second to authenticate the first user at the second device. Permit two users to manipulate their respective devices and authenticate the one first user by the second via information sent from the first device to the second.

VII Claims 23,85 125, 129:

Send to credit card information for validation at a credit card service.

VIII Claims 126-128, 130-132:

Information validation based on information sent from a first and third devices to a second device.

They are not so linked as to form a single general inventive concept (Rule 13.1 PCT) for the following reasons:

The problems solved by each group of claims are:

Group 1:

The problem solved by this group is how to authorize operations at a device without letting this device access private information.

Group 2:

The problem solved by this group of claims is how to provide credit card services.

Group 3:

The problem solved by this group of claims is how to secure communications between devices.

Group 4:

The problem solved by this group of claims is how to authenticate a user.

Group 5:

The problem solved by this group of claims is how to limit access to private information.

Group 6:

The problem solved by this group of claims is how to prevent user authentication to a device that is being manipulated by a non-trusted user.

Group 7:

The problem to be solved by this group of claims is how to validate credit card information.

Group 8:

The problem solved by this group of claims is how to validate information using a third trusted device.

The common concept linking the groups of claims listed is claim 1 and 63.

Claims 1 and 63 are not novel, as their features are anticipated by the document GB2382006A. This document shows the following features:

- a) A system for validating an identity of a user to enable or prevent an occurrence of an event (Abstract).
- b) A first device including a wireless transmitter configured to transmit validation

information (pag. 17 I.11-12, pag. 25 I.8-11 the communication between the devices is considered wireless).

- c) A second device including a wireless receiver, the second device configured to receive the validation information and further transmit the validation information (pag. 17 I.11-13, pag. 25 I.8-11 the communication between the devices is considered as wireless).
- d) A secure system in communication with the second device, the secure system including a database (pag. 17 I.10-11).
- e) The secure system is configured to receive the validation information transmitted from the second device (pag. 17 I.12-13).
- f) The secure system is further configured to transmit additional information to the second device following a receipt of the validation information to assist the second device in either enabling or preventing the occurrence of the event (pag. 17 I.15-16).

Hence the groups of claims are not so linked as to form a general inventive concept. The application lacks unity, Rule 13.1 PCT.

Re Item V.

- 1 Reference is made to the following document:
D1 : GB 2 382 006 A (IBM [US]) 14 May 2003 (2003-05-14)
D2: US 2005/001711 A1 (DOUGHTY RALPH O [US] ET AL) 6 January 2005 (2005-01-06)
- 2 The present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of claim 1 is not new in the sense of Article 33(2) PCT. Reference is made to the above reasoning of lack of unity were the novelty of claim 1 is challenged.
- 3 The same above objection is also applicable to the corresponding method claim 63 to apparatus claim 1.
- 4. The additional features of dependent claims 2-9, 13-14, 20-22 and 64-84 are also

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING
AUTHORITY (SEPARATE SHEET)**

International application No.

PCT/US2007/004646

anticipated by D1 in combination with D2, and do not contribute to an inventive activity.

Possible steps after receipt of the international search report (ISR) and written opinion of the International Searching Authority (WO-ISA)

General information	For all international applications filed on or after 01/01/2004 the competent ISA will establish an ISR. It is accompanied by the WO-ISA. Unlike the former written opinion of the IPEA (Rule 66.2 PCT), the WO-ISA is not meant to be responded to, but to be taken into consideration for further procedural steps. This document explains about the possibilities.
Amending claims under Art. 19 PCT	Within 2 months after the date of mailing of the ISR and the WO-ISA the applicant may file amended claims under Art. 19 PCT directly with the International Bureau of WIPO. The PCT reform of 2004 did not change this procedure. For further information please see Rule 46 PCT as well as form PCT/ISA/220 and the corresponding Notes to form PCT/ISA/220.
Filing a demand for international preliminary examination	<p>In principle, the WO-ISA will be considered as the written opinion of the IPEA. This should, in many cases, make it unnecessary to file a demand for international preliminary examination. If the applicant nevertheless wishes to file a demand this must be done before expiry of 3 months after the date of mailing of the ISR/ WO-ISA or 22 months after priority date, whichever expires later (Rule 54bis PCT). Amendments under Art. 34 PCT can be filed with the IPEA as before, normally at the same time as filing the demand (Rule 66.1 (b) PCT).</p> <p>If a demand for international preliminary examination is filed and no comments/amendments have been received the WO-ISA will be transformed by the IPEA into an IPRP (International Preliminary Report on Patentability) which would merely reflect the content of the WO-ISA. The demand can still be withdrawn (Art. 37 PCT).</p>
Filing informal comments	After receipt of the ISR/WO-ISA the applicant may file informal comments on the WO-ISA directly with the International Bureau of WIPO. These will be communicated to the designated Offices together with the IPRP (International Preliminary Report on Patentability) at 30 months from the priority date. Please also refer to the next box.
End of the international phase	At the end of the international phase the International Bureau of WIPO will transform the WO-ISA or, if a demand was filed, the written opinion of the IPEA into the IPRP, which will then be transmitted together with possible informal comments to the designated Offices. The IPRP replaces the former IPER (international preliminary examination report).
Relevant PCT Rules and more information	Rule 43 PCT, Rule 43bis PCT, Rule 44 PCT, Rule 44bis PCT, PCT Newsletter 12/2003, OJ 11/2003, OJ 12/2003

PATENT COOPERATION TREATY

DOCKETED
DUE: 8.10.09

PCT

7.16.09

From the INTERNATIONAL SEARCHING AUTHORITY

To:

LOWRIE, LANDO & ANASTASI LLP
Attn. Donahoe, Robert V
One Main Street
Eleventh Floor
Cambridge, MA 02142
ETATS-UNIS D'AMERIQUE

INVITATION TO PAY ADDITIONAL FEES
AND, WHERE APPLICABLE, PROTEST FEE
(PCT Article 17(3)(a) and Rule 40.1 and 40.2(e))

REGISTERED MAIL

Date of mailing (day/month/year)	10/07/2009
-------------------------------------	------------

Applicant's or agent's file reference W0537-7013WO	PAYMENT DUE within ONE MONTH from the above date of mailing
---	---

International application No. PCT/US2009/035282	International filing date (day/month/year) 26/02/2009
--	---

Applicant
WEISS, Kenneth P.

1. This International Searching Authority

- (i) considers that there are 4 (number of) inventions claimed in the international application covered by the claims indicated on an extra sheet:
- (ii) therefore considers that **the international application does not comply with the requirements of unity of invention** (Rules 13.1, 13.2 and 13.3) for the reasons indicated on an extra sheet:
- (iii) has carried out a partial international search (see Annex) will establish the international search report on those parts of the international application which relate to the invention first mentioned in claims Nos.:
see extra sheet
- (iv) will establish the international search report on the other parts of the international application only if, and to the extent to which, additional fees are paid.

2. Consequently, the applicant is hereby **invited to pay**, within the time limit indicated above, the amount indicated below:


EUR 1.700,00 x 3 = EUR 5.100
Fee per additional invention number of additional inventions currency/total amount of additional fees

3. The applicant is informed that, according to Rule 40.2(c), **the payment of any additional fee may be made under protest**, i.e., a reasoned statement to the effect that the international application complies with the requirement of unity of invention or that the amount of the required additional fee is excessive, where applicable, subject to the payment of a protest fee.

Where the applicant pays additional fees under protest, the applicant is hereby invited, within the time limit indicated above, to pay a protest fee (Rule 40.2(e)) in the amount of EUR 750,00 (currency/amount)

Where the applicant has not, within the time limit indicated above, paid the required protest fee, the protest will be considered not to have been made and the International Searching Authority will so declare.

4. Claim(s) Nos. _____ have been found to be unsearchable under Article 17(2)(b) because of defects under Article 17(2)(a) and therefore have not been included with any invention.

Name and mailing address of the International Searching Authority  European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Eva Hehn
--	------------------------------------

**Annex to Form PCT/ISA/206
COMMUNICATION RELATING TO THE RESULTS
OF THE PARTIAL INTERNATIONAL SEARCH**

International Application No
PCT/US2009/035282

1. The present communication is an Annex to the invitation to pay additional fees (Form PCT/ISA/206). It shows the results of the international search established on the parts of the international application which relate to the invention first mentioned in claims Nos.:
- see 'Invitation to pay additional fees'
2. This communication is not the international search report which will be established according to Article 18 and Rule 43.
3. If the applicant does not pay any additional search fees, the information appearing in this communication will be considered as the result of the international search and will be included as such in the international search report.
4. If the applicant pays additional fees, the international search report will contain both the information appearing in this communication and the results of the international search on other parts of the international application for which such fees will have been paid.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2006/016884 A1 (BLOCK JAMES [US] ET AL) 26 January 2006 (2006-01-26)	1-2, 4, 6, 13, 15-16, 18-28, 30-31
A	paragraph [0245] paragraph [0288] - paragraph [0290] paragraph [0026] - paragraph [0031] paragraph [0185] paragraph [0210] paragraph [0181] - paragraph [0182] paragraph [0230] figures 1, 4 paragraph [0097] - paragraph [0108] paragraph [0039] paragraph [0191] - paragraph [0192] paragraph [0023] ----- -/--	7-12, 14

Further documents are listed in the continuation of box C.

Patent family members are listed in annex.

° Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *&* document member of the same patent family

**Annex to Form PCT/ISA/206
COMMUNICATION RELATING TO THE RESULTS
OF THE PARTIAL INTERNATIONAL SEARCH**

International Application No
PCT/US2009/035282

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT		
Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	<p>US 2007/198436 A1 (WEISS KENNETH P [US]) 23 August 2007 (2007-08-23)</p> <p>paragraph [0027] paragraph [0015] paragraph [0018] paragraph [0197] paragraph [0219] paragraph [0143] paragraph [0075] figure 28 paragraph [0096]</p>	<p>1-2,4, 6-16, 18-28, 30-31</p>
A	<p>WO 96/36934 A1 (SMART TOUCH L L C [US]) 21 November 1996 (1996-11-21)</p> <p>page 6, line 32 - page 7, line 19 page 8, lines 9-13 page 8, line 31 - page 9, line 9 page 21, line 27 - page 22, line 16 page 38, lines 11-23 page 73, lines 19-26</p>	<p>1-2,4,6, 15-16, 26-28</p>
A	<p>US 2005/187843 A1 (LAPSLEY PHILIP D [US] ET AL LAPSLEY PHILIP D [US] ET AL) 25 August 2005 (2005-08-25) paragraph [0121] - paragraph [0140] paragraph [0033] paragraph [0034] paragraph [0035] paragraph [0155] - paragraph [0156]</p>	<p>1,15,20, 30-31</p>
A	<p>WO 92/07436 A1 (SECURITY DYNAMICS TECHN [US]) 30 April 1992 (1992-04-30) page 2, line 16 - page 3, line 13</p>	<p>1,15,20</p>
T	<p>WO 02/14985 A2 (KERN DANIEL A [US]) 21 February 2002 (2002-02-21) page 14, line 27 - page 15, line 7 page 1, lines 18-23 page 4, lines 9-20 claims 1,4,8 figure 12</p>	<p>1,15,20</p>

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. claims: 1-2, 4, 6-16, 18-28, 30-31

A device with biometric sensor, user interface and wireless communication interface which encrypts authentication information setup by all entered data and sends it via another device to a third party system

1.1. claims: 1-2, 4, 6, 15-16, 18-20, 24-28, 30-31

A device with biometric sensor, user interface and wireless communication interface which encrypts particular authentication information setup by all entered data and sends it via another device to a third party system

1.2. claims: 7-12

A device with biometric sensor, user interface and wireless communication interface which encrypts authentication information and sends it via another device to a third party system with local biometric verification and activation of the device after successful authentication

1.3. claim: 14

A portable device with biometric sensor, user interface and wireless communication interface which encrypts authentication information and sends it via another device to a third party system

1.4. claims: 13, 21-23

A device with a special biometric sensor, user interface and wireless communication interface which encrypts authentication information and sends it via another device to a third party system

2. claim: 3

A device with biometric sensor, user interface and wireless communication interface which encrypts authentication information and sends it via another device to a third party system and a converter device emulating magnetic stripes

3. claim: 5

A device with biometric sensor, user interface and wireless communication interface which encrypts authentication information and sends it via another device to a third party system after biometric authentication

4. claims: 17, 29

A device with biometric sensor, user interface and wireless communication interface which encrypts authentication information and sends it via another device to a third party system. The device is deactivated when user is not authenticated or when rules of other policies apply.

Please note that all inventions mentioned under item 1, although not necessarily linked by a common inventive concept, could be searched without effort justifying an additional fee.

The reasons for which the inventions are not so linked as to form a single general inventive concept, as required by Rule 13.1 PCT, are as follows:

Claims 1, 2, 15 and 20 are not new and not inventive. The only common feature linking the parallel claims 3, 4, 5, 6, 7, 13, 14, 16, 17, 18, 19, 21, 24, 25, 29 and 30 is a device with biometric sensor, user interface and wireless communication interface which encrypts authentication information setup by all entered data and sends it via another device to a third party system

This is disclosed by the document US2006016884 (the references in parentheses applying to this document):

A device configured to allow a user to select any one of a plurality of accounts associated with the user to employ in a financial transaction (fig.1 "portable terminal 14"; fig. 4; par.[0245] "a multifunction card can store data corresponding to plurality of accounts in its memory. ..., data corresponding to a stored account can be selected ..."), comprising: a biometric sensor configured to receive a biometric input provided by the user (fig.4 "BIOMETRIC READER 47"); a user interface (fig. 4 "40 DISPLAY", "42 MANUAL INPUTS") configured to receive a user input including secret information known to the user and identifying information concerning an account selected by the user from the plurality of accounts (par.[0181] "The instructions stored in memory on the card or the memory of the terminal may cause screens associated with the entry of a PIN number and/or the selection of various accounts to be displayed when particular accounts are selected."); a communication link (fig.4 "50 MODEM") configured to communicate (fig.4 "54") with a secure registry (fig.4 "56"); and a processor (fig.4 "36 PROCESSOR") coupled to the biometric sensor to receive information concerning the biometric input, the user interface and the communication link, the processor configured to generate a non-predictable value and to generate encrypted authentication information from the non-predictable value, the identifying information, and at least one of the information concerning the biometric input and the secret information, and to communicate the encrypted authentication information via the communication link to the secure registry (par.[0185] "Appropriate encryption is provided to enhance security."; par.[0191]-[0192] "Data representative of the user's signature and/or the user's financial account information can be transmitted from the user's (customer's) portable hand-held device to the merchant's transaction system. ... , the merchant system can be operative to communicate with a third party ... the account data may include checking account number

(and/or bank routing number), check number, name, address, phone number, bank name, or combinations thereof.").

The 6 groups of inventions are directed towards the solution of different technical problems and are not linked by a common or corresponding special technical feature, problem or effect, which would contribute to the prior art.

Claims 1, 2, 4, 6, 15, 16, 18 to 20, 24 to 28, 30, 31 are directed towards a device for entering authentication data and generating encrypted authentication information to be communicated to a third party. The problem to be solved by these features can be construed as to protecting the secrecy of data authorizing financial transactions.

Claims 7 to 12 are directed towards authenticating the authorized user of the device locally. Claim 14 is directed towards a portable authentication device. The problem to be solved by these features can be construed as to improve the availability of the protected authentication. Hence two solutions form a common inventive concept.

Claims 13, 21, 22, 23 are directed towards biometric sensors. The problem to be solved by these features can be construed as to increase convenience for the user.

Claim 3 is directed towards a device for emulating magnetic stripes. The problem to be solved by these features can be construed as to improve the interoperability with existing authentication systems.

Claim 5 is directed towards sending biometric information to a third party before authenticating the financial transaction. The problem to be solved by these features can be construed as to improve the secrecy of the authentication process.

Claim 17 and 29 are directed towards restricting the usage of the device. The problem to be solved by these features can be construed as to protect the integrity of the device against unauthorized use.

In conclusion, the groups of claims define 6 different inventions not linked by a single general inventive concept.

The search has covered the first 4 groups of inventions (groups 1, 1.1, 1.2, 1.3).

Patent Family Annex

Information on patent family members

International Application No

PCT/US2009/035282

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
US 2006016884	A1	26-01-2006	NONE	
US 2007198436	A1	23-08-2007	US 2007289000 A1 US 2007288758 A1	13-12-2007 13-12-2007
WO 9636934	A1	21-11-1996	AT 254315 T AU 5922696 A BR 9608580 A CA 2221321 A1 CN 1191027 A CN 1542680 A DE 69630713 D1 DE 69630713 T2 DK 0912959 T3 EP 0912959 A1 ES 2213774 T3 HK 1069655 A1 JP 11511882 T JP 4097040 B2 JP 2006155628 A JP 2006146945 A JP 2007293878 A JP 2009087379 A PT 912959 E	15-11-2003 29-11-1996 05-01-1999 21-11-1996 19-08-1998 03-11-2004 18-12-2003 02-12-2004 15-03-2004 06-05-1999 01-09-2004 25-01-2008 12-10-1999 04-06-2008 15-06-2006 08-06-2006 08-11-2007 23-04-2009 31-05-2004
US 2005187843	A1	25-08-2005	NONE	
WO 9207436	A1	30-04-1992	AU 649190 B2 AU 7981691 A CA 2094026 A1 DE 69133047 D1 DE 69133047 T2 DE 555219 T1 EP 0555219 A1 JP 6507277 T	12-05-1994 20-05-1992 20-04-1992 01-08-2002 14-11-2002 28-11-1996 18-08-1993 11-08-1994
WO 0214985	A2	21-02-2002	AU 8344701 A BR 0113462 A CA 2419566 A1 CN 1459068 A EP 1323011 A2 JP 2004506973 T MX PA03001461 A	25-02-2002 30-12-2003 21-02-2002 26-11-2003 02-07-2003 04-03-2004 13-12-2004

Electronic Patent Application Fee Transmittal

Application Number:	11768729
Filing Date:	26-Jun-2007
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Filer:	Robert Vincent Donahoe
Attorney Docket Number:	W0537-7006

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 1 month with \$0 paid	2251	1	65	65

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Submission- Information Disclosure Stmt	1806	1	180	180
Total in USD (\$)				245

Electronic Acknowledgement Receipt

EFS ID:	9897412
Application Number:	11768729
International Application Number:	
Confirmation Number:	3536
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Correspondence Address:	John N. Anastasi c/o Lowrie, Lando & Anastasi, LLP Riverfront Office Park, One Main Street - Cambridge MA 02142 US 6173957000 -
Filer:	Robert Vincent Donahoe
Filer Authorized By:	
Attorney Docket Number:	W0537-7006
Receipt Date:	18-APR-2011
Filing Date:	26-JUN-2007
Time Stamp:	16:06:47
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$245

RAM confirmation Number	2519
Deposit Account	502762
Authorized User	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		W0537-700620_Response.pdf	39175 2e166cbecad982c11d7426d0827184d44837785c	yes	5

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment/Req. Reconsideration-After Non-Final Reject	1	1
Applicant Arguments/Remarks Made in an Amendment	2	5

Warnings:

Information:

2	Transmittal Letter	W0537-700620_IDS_Transmittal.pdf	30180 4051f6d2d78333b52e5627e361dea20791d74ee7	no	3
---	--------------------	----------------------------------	---	----	---

Warnings:

Information:

3	Information Disclosure Statement (IDS) Filed (SB/08)	W0537-700620_IDS.pdf	612927 ed86332543e6e8e6e15b1979277e736ba753a650	no	5
---	--	----------------------	--	----	---

Warnings:

Information:

4	Foreign Reference	EP1081632A1.pdf	815154 c64904ebfc0e065a78dbd44d668533c7a89d0853	no	15
---	-------------------	-----------------	--	----	----

Warnings:

Information:

5	Foreign Reference	GB2382006.pdf	2167939 40cb9cd97fb222e4eea10e8a4cb9c191d37ce767	no	53
---	-------------------	---------------	---	----	----

Warnings:

Information:

6	Foreign Reference	WO1992007436.pdf	859097 7a6c1113a3c42bd3d4f298d6e166dd9ac135f8cc	no	25
---	-------------------	------------------	--	----	----

Warnings:

Information:

7	NPL Documents	NPL_FIPS_PUB.pdf	9275	no	1
			afc3e6f3952231a61e19e11b090d6059d43c3658		
Warnings:					
Information:					
8	NPL Documents	NPL_Introduction_Cryptography.pdf	109484	no	1
			9d5bebd6f60d9eb29cb77e9d43354b03ba7cec5		
Warnings:					
Information:					
9	NPL Documents	PCT_US2007_070701.pdf	623149	no	13
			49706562019ba4f5e76d2dfdc49f7c605ed0baa1		
Warnings:					
Information:					
10	NPL Documents	PCT_US2007_004646.pdf	737062	no	17
			0ee126137270f4fed4820a8444d2544d52484eb3		
Warnings:					
Information:					
11	NPL Documents	PCT_US2009_035282.pdf	392014	no	7
			66d86d8c5f84e6d28dc59db6e4dff3c148783b54		
Warnings:					
Information:					
12	NPL Documents	Biometrics.pdf	320463	no	5
			97108e1864bbc1a7e3d61f7e851ee841ead9950		
Warnings:					
Information:					
13	Fee Worksheet (PTO-875)	fee-info.pdf	32043	no	2
			4825caa4c63b3f093f9627dea2d770e10f46eaaad		
Warnings:					
Information:					
Total Files Size (in bytes):			6747962		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/768,729	06/26/2007	Kenneth P. Weiss	W0537-7006	3536

7590 06/29/2011
John N. Anastasi
c/o Lowrie, Lando & Anastasi, LLP
Riverfront Office Park, One Main Street
Cambridge, MA 02142

EXAMINER

DADA, BEEMNET W

ART UNIT	PAPER NUMBER
----------	--------------

2435

MAIL DATE	DELIVERY MODE
-----------	---------------

06/29/2011

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

DETAILED ACTION

This office action is in reply to an amendment filed on 04/18/2011. Claims 1-5, 9-16, 18-21, 24-30, 32-39 and 41-45 are pending.

Response to Arguments

Applicant's arguments filed 04/18/2011 have been fully considered but they are not persuasive. Applicant argues that the prior art on record fails to teach the limitation "mapping the time varying multicharacter code to information required to provide the services" Examiner disagrees.

Examiner would point out that, Gioradano teaches a method/system configured to map the multi-character code to secure data including information required to provide the services, the information including account identifying information where the account identifying information is unknown to the service provider, to provide the account identifying information to a third party to enable a transaction without providing the account identifying information to the service provider (i.e., note that the POS system does not get access to customers credit/debit account information, column 18, lines 5-47). Gioradano is silent on the multi-character code being time-varying. However, Brainard teaches an authentication system that maps time-varying multi-character code to stored secure data (i.e., verifying by comparing an authentication code, wherein the authentication code is time dependent, paragraphs 0019, 0020, 0045 and 0063). Examiner would further point out that, the time varying multi-character code of Brainard can be implemented into the multi-character code of Gioradano in order to enhance security of the system by changing the code based on timing data. It is therefore, the combination of Gioradano and Brainard that teaches the limitation mapping a time-varying multi-character code

Art Unit: 2435

to secure data ... unknown to the service provider. Examiner would further point out that the art on record teaches the claim limitations and therefore, the rejection is respectfully maintained.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1-5, 9-16, 18-21, 24-30, 32-39 and 41-45 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gioradano et al. US 7,571,139 B1 (hereinafter Gioradano) in view Brainard et al. US 2006/0256961 A1 (hereinafter Brainard).

As per claims 1 and 16, Giorandano teaches a secure registry system for providing information to a service provider to enable the service provider to provide services to entities with secure data stored in the secure registry system, comprising:

a database including secure data for each entity, wherein each entity is associated with and a multicharacter_code for each entity having secure data in the secure registry system, respectively [column 18, lines 14-47] and

a processor configured to receive, from the service provider, the multicharacter code for the entity on whose behalf services are to be provided, configured to map the multicharacter code to secure data including information required to provide the services, the information including account identifying information where the account identifying information is unknown to the service provider, to provide the account identifying information to a third party to enable a transaction without providing the account identifying information to the service provider (i.e.,

Art Unit: 2435

note that the POS system does not get access to customers credit/debit account information, column 18, lines 5-47). Gioradano does not explicitly teach a time-varying code. In the same field of endeavor, Brainard teaches an authentication system including a time-varying multicharacter code to secure data and data access [paragraphs 0019 and 0020]. It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Brainard within the system of Gioradano in order to enhance the security of the system.

As per claims 2 and 18, Gioradano further teaches the system wherein the multicharacter code represents an identity of the entity [column 18, lines 14-47].

As per claims 3 and 19, Gioradano further teaches the system wherein the multicharacter code is provided to the system via a secure electronic transmission device [column 18, lines 14-47].

As per claim 4 and 20, Gioradano further teaches the system wherein the code is encrypted and transmitted to the system and wherein the system is configured to decrypt the code with a public key of the entity [column 18, lines 14-47].

As per claims 5 and 21, Gioradano further teaches the system wherein said service provider's service includes delivery, wherein the information is an address to which an item is to be delivered to the entity, wherein the system receives the code and wherein the system uses the code to obtain the appropriate address for delivery of the item by the third party [column 18, lines 14-47].

As per claim 9-15, 41-45, 24-27, 30, 32 and 41-45 Gioradano further teaches the system wherein the account identifying information includes credit card information regarding the entity and the processor is configured to provide the credit card information based upon the code of the entity to enable the transaction [column 18, lines 14-47].

As per claims 28-29 and 33-39, Gioradano further teaches the system wherein the database is further configured to associate biometric information with each entity having secure data in the secure registry respectively [column 18, lines 14-47].

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.


Any inquiry concerning this communication or earlier communications from the examiner should be directed to BEEMNET DADA whose telephone number is (571)272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

Art Unit: 2435

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BEEMNET DADA/
Primary Examiner, Art Unit 2435

Search Notes 	Application/Control No. 11768729	Applicant(s)/Patent Under Reexamination WEISS, KENNETH P.
	Examiner BEEMNET W DADA	Art Unit 2435

SEARCHED			
Class	Subclass	Date	Examiner
713	169, 182, 184	6/27/11	BD
707	9	6/27/11	BD

SEARCH NOTES		
Search Notes	Date	Examiner
East search	6/27/11	BD
NPL search	6/27/11	BD
Inventor name search	6/27/11	BD

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

--	--

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11768729
	Filing Date	2007-06-27
	First Named Inventor	Kenneth P. Weiss
	Art Unit	2435
	Examiner Name	Dada, Beemnet W.
	Attorney Docket Number	W0537-700620

U.S.PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1	6309342		2001-10-30	Blazey et al.		
	2	6819219		2004-11-16	Bolle et al.		

If you wish to add additional U.S. Patent citation information please click the Add button.

Add

U.S.PATENT APPLICATION PUBLICATIONS							Remove
Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	
	1						

If you wish to add additional U.S. Published Application citation information please click the Add button.

Add

FOREIGN PATENT DOCUMENTS								Remove
Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² j	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	1 081 632	EP		2001-07-03	Keyware Technologies		<input type="checkbox"/>
	2	2 382 006	GB		2003-05-14	IBM		<input type="checkbox"/>

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number	11768729
	Filing Date	2007-06-27
	First Named Inventor	Kenneth P. Weiss
	Art Unit	2435
	Examiner Name	Dada, Beemnet W.
	Attorney Docket Number	W0537-700620

3	1992007436	WO		1992-04-30	Security Dynamics Limited, Inc.	<input type="checkbox"/>
---	------------	----	--	------------	---------------------------------	--------------------------

If you wish to add additional Foreign Patent Document citation information please click the Add button

NON-PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	"FIPS PUB 46-3." 25 October 1999. National Institute of Science and Technology (NIST).	<input type="checkbox"/>
	2	"PGP: An Introduction to Cryptography." 2000.	<input type="checkbox"/>
	3	International Search Report from PCT/US2007/070701 mailed March 11, 2008.	<input type="checkbox"/>
	4	International Search Report from PCT/US2007/004646 mailed November 27, 2007.	<input type="checkbox"/>
	5	International Search Report from PCT/US2009/035282 mailed July 10, 2009.	<input type="checkbox"/>
	6	Pabrai, U. "Biometrics for PC-User Authentication: A Primer" 1 February 2001. Access Controls & Security Systems. All pages. < http://www.securitysolutions.com/mag/security_biometrics_pcuser_authentication/index.html >	<input type="checkbox"/>

If you wish to add additional non-patent literature document citation information please click the Add button

EXAMINER SIGNATURE

Examiner Signature	/Beemnet Dada/	Date Considered	06/27/2011
--------------------	----------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BD/

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	11768729
Filing Date	2007-06-27
First Named Inventor	Kenneth P. Weiss
Art Unit	2435
Examiner Name	Dada, Beemnet W.
Attorney Docket Number	W0537-700620

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL (Submitted Only via EFS-Web)

Application Number	11768729	Filing Date	2007-06-26	Docket Number (if applicable)	W0537-700620	Art Unit	2435
First Named Inventor	Kenneth P. Weiss			Examiner Name	B. W. Dada		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
 Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

Other _____

Enclosed

Amendment/Reply

Information Disclosure Statement (IDS)

Affidavit(s)/ Declaration(s)

Other

 Petition for Two Month Extension of Time

MISCELLANEOUS

Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____
 (Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

Other _____

FEES

The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.

The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 50/2762

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Patent Practitioner Signature

Applicant Signature

Signature of Registered U.S. Patent Practitioner			
Signature	/Robert V. Donahoe/	Date (YYYY-MM-DD)	2011-11-29
Name	Robert V. Donahoe	Registration Number	46667

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with 37 CFR § 1.6(a)(4).

Dated: November 29, 2011
Electronic Signature for Robert V. Donahoe: /Robert V. Donahoe/

Docket No.: W0537-700620
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Kenneth P. Weiss

Application No.: 11/768,729

Confirmation No.: 3536

Filed: June 26, 2007

Art Unit: 2435

For: UNIVERSAL SECURE REGISTRY

Examiner: B. W. Dada

AMENDMENT AFTER FINAL ACTION UNDER 37 C.F.R. 1.116

MS RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

In response to the final Office Action mailed June 29, 2011, please amend the above-identified application as follows. Changes to the Claims are shown by strike through (for deleted matter) and underlining (for added matter).

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks begin on page 9 of this paper.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A secure registry system for providing information to a first party~~service provider~~ to enable transactions between the first party and the service provider to ~~provide services to~~ entities with secure data stored in the secure registry system, the secure registry system comprising:

a database including secure data for each entity, wherein each entity is associated with a time-varying multicharacter code for each entity having secure data in the secure registry system, respectively, each time-varying multicharacter code representing an identity of one of the respective entities; and

a processor configured to receive, from the first party~~service provider~~, the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed~~services are to be provided~~, configured to map the time-varying multicharacter code to the identity of the entity and secure data associated with the entity including information required to enable~~provide~~ the transactions~~services~~, the information including account identifying information where the account identifying information is unknown to the first party~~service provider~~, to provide the account identifying information to a third party to enable the~~the~~ transaction without providing the account identifying information to the first party~~service provider~~.

2. (Canceled)

3. (Previously Presented) The system of claim 1, wherein the time-varying multicharacter code is provided to the system via a secure electronic transmission device.

4. (Previously Presented) The system of claim 1, wherein the time-varying multicharacter code is encrypted and transmitted to the system, and

wherein the system is configured to decrypt the time-varying multicharacter code with a public key of the entity.

5. (Currently Amended) The system as claimed in claim 1, wherein the transaction includes a service provided by the first party,

wherein said first party's service provider's service includes delivery,

wherein the information is an address to which an item is to be delivered to the entity,

wherein the system receives the time-varying multicharacter code, and

wherein the system uses the time-varying multicharacter code to obtain the appropriate address for delivery of the item by the third party.

6. (Canceled).

7. (Canceled).

8. (Canceled).

9. (Previously Presented) The secure registry system as claimed in claim 1, wherein the account identifying information includes credit card account information regarding the entity, and wherein the processor is configured to provide the credit card account information based upon the multicharacter code of the entity to enable the transaction.

10. (Previously Presented) The system as claimed in claim 9, wherein the system is configured to receive an approval of the credit card transaction.

11. (Previously Presented) The system as claimed in claim 1, wherein the account identifying information includes bank card account information regarding the entity, and wherein the processor is configured to provide the bank card account information to enable the transaction based upon the multicharacter code of the entity.

12. (Previously Presented) The system as claimed in claim 11, wherein the system is configured to provide an approval of the bank card transaction.

13. (Previously Presented) The system as claimed in claim 1, wherein the information includes personal identification information regarding the entity.

14. (Currently Amended) The system as claimed in claim 13, wherein the personal identification information comprises a photograph of the entity, and wherein the photograph is provided to the first party~~service provider~~.

15. (Previously Presented) The system as claimed in claim 1, wherein the account identifying information identifies email address information regarding the entity.

16. (Currently Amended) A method for providing information to a first party to enable transactions a service to between the first party and entities who have secure data stored in a secure registry in which each entity is identified by a time-varying multicharacter code, ~~the service provided by a service provider~~, the method comprising:

receiving the time-varying multicharacter code for an entity on whose behalf a transaction is to take place~~the services are to be provided~~;

mapping the time-varying multicharacter code to an identity of the entity and information required to perform the transaction~~provide the services~~, the information including account identifying information unknown to the first party~~service provider~~;

providing the account identifying information to a third party without providing the account identifying information to the first party~~service provider~~; and

using the account identifying information to enable the first party~~service provider~~ to perform~~provide~~ the transaction~~service~~ without the first party's~~service provider's~~ knowledge of the account identifying information.

17. (Canceled).

18. (Canceled)

19. (Previously Presented) The method of claim 16, wherein the act of receiving the time-varying multicharacter code comprises receiving the time-varying multicharacter code transmitted via a secure electronic transmission device.

20. (Previously Presented) The method of claim 16, wherein the act of receiving the time-varying multicharacter code comprises receiving an encrypted multicharacter code, and wherein the method further comprises decrypting the encrypted multicharacter code.

21. (Currently Amended) The method as claimed in claim 16, wherein the transaction includes a service provided by the first party, provider's service wherein the service includes delivery,
wherein the account identifying information is associated with an address to which an item is to be delivered for the entity, and
wherein the third party receives the address for delivery of an item provided by the first party service provider.

22. (Canceled).

23. (Canceled).

24. (Currently Amended) The method as claimed in claim 16, wherein the account identifying information includes a credit card number, and wherein the act of using the account identifying information ~~to perform the services~~ comprises using the credit card number to enable the[[a]] transaction.

25. (Currently Amended) The method as claimed in claim 24, wherein the act of using the account identifying information comprises receiving a validation or denial of the transaction without providing the credit card number of the entity to the first party service provider.

26. (Currently Amended) The method as claimed in claim 16, wherein the act of using the account identifying information to ~~perform the services~~ comprises using bank card information about the entity to enable a transaction.

27. (Currently Amended) The method as claimed in claim 26, wherein the act of using the information comprises receiving a validation or denial of the bank card transaction without providing a bank card number of the entity to the first party service provider.

28. (Currently Amended) The method as claimed in claim 16, wherein the act of mapping the time-varying multicharacter code to information required by the first party service provider comprises mapping the time-varying multicharacter code to personal identification information about the entity.

29. (Currently Amended) The method as claimed in claim 28, wherein the personal identification information comprises a photograph of the entity, and
wherein the method further comprises an act of providing the photograph to the first party service provider.

30. (Previously Presented) The method as claimed in claim 16, wherein the account identifying information identifies email address information about the entity.

31. (Canceled).

32. (Currently Amended) The method as claimed in claim 24, further comprising an act of transmitting to the first party service provider one of an approval or a denial of the credit card transaction.

33. (Previously Presented) The system of claim 1, wherein the database is further configured to associate biometric information with each entity having secure data in the secure registry, respectively.

34. (Currently Amended) The system of claim 33, wherein the processor is further configured to map the time-varying multicharacter code to biometric information associated with the entity on whose behalf the transaction is to be performed~~services are to be provided~~ and to provide the biometric information to the first party~~service provider~~.

35. (Currently Amended) The system of claim 34, wherein the biometric information includes an image of the entity on whose behalf the transaction is to be performed~~services are to be provided~~.

36. (Currently Amended) The system of claim 34, wherein the time-varying multicharacter code is generated by a device associated with the entity on whose behalf the transaction is to be performed~~services are to be provided~~.

37. (Previously Presented) The method as claimed in claim 16, further comprising an act of associating biometric information with each entity having secure data in the secure registry, respectively.

38. (Currently Amended) The method of claim 37, further comprising acts of: mapping the time-varying multicharacter code to biometric information associated with the entity on whose behalf the transaction is to be performed~~services are to be provided~~; and providing the biometric information to the first party~~service provider~~.

39. (Currently Amended) The method of claim 38, wherein the biometric information includes an image of the entity on whose behalf the transaction is to be performed~~services are to be provided~~.

40. (Canceled).

41. (Previously Presented) The secure registry system of claim 1, wherein the account identifying information includes an account number.

42. (Previously Presented) The secure registry system of claim 41, wherein the account identifying information includes credit card account information and the account number includes a credit card number.

43. (Previously Presented) The secure registry system of claim 41, wherein the third party includes a financial service provider and the account number includes at least one of a debit card number and a credit card number.

44. (Currently Amended) The secure registry of claim 43, wherein the first ~~partyservice provider~~ includes a merchant, and the service includes a sale of at least one of goods and services.

45. (Currently Amended) The secure registry system of claim 44, wherein the processor is further configured to receive, from the first ~~partyservice provider~~, a merchant ID, and a purchase amount.

46. (New) The secure registry system of claim 1, wherein the identity of the entity is unknown until the time-varying code is mapped to the identity by the processor.

REMARKS

Claims 1-5, 9-16, 18-21, 24-30, 32-39 and 41-45 were previously pending in this application. with claims 1 and 16 being independent claims. By this amendment, Applicant is canceling claims 2 and 18 without prejudice or disclaimer. Claims 1, 5, 16, 21, 24-29, 32, 34-36, 38, 39, 44 and 45 are amended. New claim 46 is added herein. As a result claims 1, 2-5, 9-16, 19-21, 24-30, 32-39 and 41-46 are pending for examination with claims 1 and 16 being independent claims. No new matter has been added. Support for the amendments can be found in the originally-filed application in Fig. 10 and the associated description at page 19, line 22 to page 20, line 16, for example.

Rejections Under 35 U.S.C. §103(a)

The Office Action rejects claims 1-5, 9-16, 18-21, 24-30, 32-39 and 41-45 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 7,571,139 to Gioradano (hereinafter Gioradano) in view of U.S. Patent No. 2006/0256961 to Brainard (hereinafter Brainard). Applicant respectfully asserts that that claims as amended herein are patentable in view of the cited references at least because Giordano and Brainard alone or in proper combination do not teach or suggest “a processor configured to receive, from the first party, the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed, configured to map the time-varying multicharacter code to the identity of the entity and secure data associated with the entity including information required to enable the transaction, the information including account identifying information where the account identifying information is unknown to the first party, to provide the account identifying information to a third party to enable the transaction without providing the account identifying information to the first party,” as recited in claim 1, for example.

For example, the originally-filed application describes that a “user initiates an *anonymous* purchase by entering a secret code into the electronic ID device and transmit[s] the results to the on-line merchant.” The description further provides that “the *merchant transmits this information to the USR software 18, along with the store number and the amount of the purchase.*” As a result, approaches described in the application result in a “secure registry” receiving information to enable a “transaction” where the identity of the entity “on whose behalf

the transaction is to be performed” is anonymous until “the time-varying multicharacter code [is mapped] to the identity of the entity.”

In contrast, Giordano only teaches approaches in which static information must be provided. For example, a “customer transceiver 50 is programmed with *the customer’s ID number* in step 370, the customer transceiver 50 is mailed to the customer in step 380.” Further, the “customer transceiver 50 consists of an electronic transmitter/receiver combination including a unique customer/transmitter ID number programmed therein.” Giordano teaches that when the customer transceiver interfaces with the merchant transceiver “a *customer identification signal including the unique customer/transmitter ID number is transmitted to the merchant transceiver* 48.” (col. 17, lines 28-59.) Accordingly, in Giordano operation of the system requires that the customer ID number provide the identification. Unlike a time-varying code, the customer ID in Giordano is static and provides an identification that is matched to an index of static values without requiring any additional measures. Although the system 10 does not provide the customer’s credit card to the sales associate, it remains vulnerable to identity theft because the customer ID number is a static piece of information that can be intercepted and later used by an imposter.

The Examiner admits and Applicant agrees that “Giordano does not explicitly teach a time-varying code.” (Office Action at page 4.) Instead, the Office Action relies on Brainard for an alleged teaching of “an authentication system including a time-varying code.” *Id.* Applicant respectfully notes that Brainard does not cure the deficiencies of Giordano because, in Brainard, the user necessarily also provides a static identification that is used by a verifier. In particular, “the verifier 221 determines whether the code is appropriate, for example, whether it is, in the above embodiment, correctly derived from the verifier seed, the user’s PIN and the current time.” (Paragraph 0058) As taught in Brainard, the verifier 221 necessarily must know the purported identity of the user to determine whether the code was correctly derived.

Thus, independent claims 1 and 16 are patentable at least because Giordano and Brainard alone or in proper combination do not teach or suggest an approach where a “secure registry” receives information to enable a “transaction” where the identity of the entity “on whose behalf the transaction is to be performed” is anonymous until “the time-varying multicharacter code [is mapped] to the identity of the entity.” Claims 2 and 18 are canceled herein. Each of claims 3-5, 9-15, 19-21, 24-30, 32-39 and 41-45 depend from one of the allowable independent claims and

is patentable for at least the same reasons. Accordingly, reconsideration and withdrawal of this rejection is respectfully requested.

CONCLUSION

In view of the foregoing amendments and remarks, reconsideration is respectfully requested. This application should now be in condition for allowance; a notice to this effect is respectfully requested. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicant's attorney at the telephone number listed below.

A Request for Continued Examination and a fee for a two month extension of time are included herewith. If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee that is not covered by an accompanying payment, please charge any deficiency to Deposit Account No. 50/2762, Ref. No. W0537-700620.

Dated: November 29, 2011

Respectfully submitted,

Electronic signature: /Robert V. Donahoe/
Robert V. Donahoe

Registration No.: 46,667
LANDO & ANASTASI LLP
Riverfront Office Park
One Main Street
Suite 1100
Cambridge, Massachusetts 02142
(617) 395-7000
Attorney for Applicant

Electronic Patent Application Fee Transmittal

Application Number:	11768729
Filing Date:	26-Jun-2007
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Filer:	Robert Vincent Donahoe
Attorney Docket Number:	W0537-7006

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 2 months with \$0 paid	2252	1	280	280

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Request for continued examination	2801	1	465	465
Total in USD (\$)				745

Electronic Acknowledgement Receipt

EFS ID:	11502418
Application Number:	11768729
International Application Number:	
Confirmation Number:	3536
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Correspondence Address:	John N. Anastasi c/o Lowrie, Lando & Anastasi, LLP Riverfront Office Park, One Main Street - Cambridge MA 02142 US 6173957000 -
Filer:	Robert Vincent Donahoe
Filer Authorized By:	
Attorney Docket Number:	W0537-7006
Receipt Date:	29-NOV-2011
Filing Date:	26-JUN-2007
Time Stamp:	17:18:27
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$745

RAM confirmation Number		5605			
Deposit Account		502762			
Authorized User					
File Listing:					
Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Extension of Time	W0537-700620_- _Petition_for_Extension_of_Ti me_Under_37_CFR_1136a_1. PDF	22310 159ce447853c91f97cc5d1e5405c9cd8d02 a6c7	no	2
Warnings:					
Information:					
2	Request for Continued Examination (RCE)	W0537-700620_- _Request_for_Continued_Exa mination_Fillable_PDF_2.pdf	697783 d7cd86256279f4ba7c106a4c5fc6cd4741ab b1ea	no	3
Warnings:					
Information:					
3		W0537-700620_- _Amendment_After_Final_3. PDF	68732 603ddc378c9809f198900f5fbd430f9414b d6e4	yes	11
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Amendment After Final		1	1	
	Claims		2	8	
	Applicant Arguments/Remarks Made in an Amendment		9	11	
Warnings:					
Information:					
4	Fee Worksheet (SB06)	fee-info.pdf	32166 c00e52739b5e0344cc03b9e61ac9e5dfd03f e74e	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			820991		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with 37 CFR § 1.6(a)(4).

Dated: November 29, 2011
Electronic Signature for Robert V. Donahoe: /Robert V. Donahoe/

Docket No.: W0537-700620
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Kenneth P. Weiss

Application No.: 11/768,729

Confirmation No.: 3536

Filed: June 26, 2007

Art Unit: 2435

For: UNIVERSAL SECURE REGISTRY

Examiner: B. W. Dada

REQUEST FOR EXTENSION OF TIME

MS RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicant hereby petitions for a two month extension of time to and including November 29, 2011 to respond to the Office Action mailed June 29, 2011.

In the event that a further petition for an extension of time is required to be submitted at this time, applicant hereby petitions under 37 C.F.R. § 1.136(a) for an extension of time for as many months as are required to ensure that the above-identified application does not become abandoned.

Please charge our Deposit Account No. 50/2762 in the amount of \$745.00 covering the fees set forth in 37 CFR 1.17(e) and 1.17(a)(2). The Director is hereby authorized to charge any deficiency in the fees filed, asserted to be filed or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to our Deposit Account No. 50/2762, under Order No. W0537-700620.

Dated: November 29, 2011

Respectfully submitted,

Electronic signature: /Robert V. Donahoe/

Robert V. Donahoe

Registration No.: 46,667

LANDO & ANASTASI LLP

Riverfront Office Park

One Main Street

Suite 1100

Cambridge, Massachusetts 02142

(617) 395-7000

Attorney for Applicant

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 11/768,729	Filing Date 06/26/2007	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

APPLICATION AS FILED – PART I			OTHER THAN SMALL ENTITY				
(Column 1)		(Column 2)	SMALL ENTITY <input checked="" type="checkbox"/>		OR	SMALL ENTITY	
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)		RATE (\$)	FEE (\$)
<input type="checkbox"/> BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>	N/A	N/A	N/A			N/A	
<input type="checkbox"/> SEARCH FEE <small>(37 CFR 1.16(k), (j), or (m))</small>	N/A	N/A	N/A			N/A	
<input type="checkbox"/> EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A	N/A			N/A	
TOTAL CLAIMS <small>(37 CFR 1.16(j))</small>	minus 20 =	*	X \$ =		OR	X \$ =	
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>	minus 3 =	*	X \$ =			X \$ =	
<input type="checkbox"/> APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.16(j))</small>							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY					
(Column 1)		(Column 2)	(Column 3)		SMALL ENTITY		OR	SMALL ENTITY		
AMENDMENT	11/29/2011	CLAIMS REMAINING AFTER AMENDMENT	MINUS	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)		RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	* 36	Minus	** 37	= 0	X \$30 =	0	OR	X \$ =	
	Independent <small>(37 CFR 1.16(h))</small>	* 2	Minus	***3	= 0	X \$125 =	0	OR	X \$ =	
<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>										
<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>								OR		
					TOTAL ADD'L FEE	0		OR	TOTAL ADD'L FEE	

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY				
(Column 1)		(Column 2)	(Column 3)		SMALL ENTITY		OR	SMALL ENTITY	
AMENDMENT	CLAIMS REMAINING AFTER AMENDMENT	MINUS	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)		RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	*	Minus	**	=	X \$ =		OR	X \$ =
	Independent <small>(37 CFR 1.16(h))</small>	*	Minus	***	=	X \$ =		OR	X \$ =
<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>									
<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>								OR	
					TOTAL ADD'L FEE			OR	TOTAL ADD'L FEE

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
 ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
 *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
 The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
 /PARTHENIA D. MERRILL/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/768,729	06/26/2007	Kenneth P. Weiss	W0537-7006	3536

7590 03/06/2012
 John N. Anastasi
 c/o Lowrie, Lando & Anastasi, LLP
 Riverfront Office Park, One Main Street
 Cambridge, MA 02142

EXAMINER

DADA, BEEMNET W

ART UNIT	PAPER NUMBER
2435	

MAIL DATE	DELIVERY MODE
03/06/2012	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 11/768,729	Applicant(s) WEISS, KENNETH P.	
	Examiner BEEBNET DADA	Art Unit 2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) Responsive to communication(s) filed on 29 November 2011.
- 2a) This action is **FINAL**.
- 2b) This action is non-final.
- 3) An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
- 4) Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 5) Claim(s) 1,3-5,9-16,19-21,24-30,32-39 and 41-46 is/are pending in the application.
- 5a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 6) Claim(s) _____ is/are allowed.
- 7) Claim(s) 1,3-5,9-16,19-21,24-30,32-39 and 41-46 is/are rejected.
- 8) Claim(s) _____ is/are objected to.
- 9) Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 10) The specification is objected to by the Examiner.
- 11) The drawing(s) filed on _____ is/are: a) accepted or b) objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 12) The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 13) Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
a) All b) Some * c) None of:
1. Certified copies of the priority documents have been received.
2. Certified copies of the priority documents have been received in Application No. _____.
3. Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) Notice of References Cited (PTO-892)
- 2) Notice of Draftperson's Patent Drawing Review (PTO-948)
- 3) Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.
- 4) Interview Summary (PTO-413)
Paper No(s)/Mail Date _____.
- 5) Notice of Informal Patent Application
- 6) Other: _____.

DETAILED ACTION

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 11/29/2011 has been entered. Claims 1, 5, 16, 21, 24-29, 32, 34-36, 38, 39, 44 and 45 have been amended and new claim 46 has been added. Claims 1, 3-5, 9-16, 19-21, 24-30, 32-39 and 41-45 are pending.

Response to Arguments

Applicant's arguments filed 11/29/2011 have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 3-5, 9-16, 19-21, 24-30, 32-39 and 41-46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gioradano et al. US 7,571,139 B1 (hereinafter Gioradano) in view Hsiao US 5,971,272.

Art Unit: 2435

As per claims 1 and 16, Giorandano teaches a secure registry system for providing information to a service provider to enable the service provider to provide services to entities with secure data stored in the secure registry system, comprising:

a database including secure data for each entity, wherein each entity is associated with and a multicharacter_code for each entity having secure data in the secure registry system, respectively [column 18, lines 14-47] and

a processor configured to receive, from the first party, the multicharacter code for the entity on whose behalf of a transaction is to be performed, configured to map the multicharacter code to the identity of the entity and secure data associated with the entity including information required to enable the transaction, the information including account identifying information where the account identifying information is unknown to the first party, to provide the account identifying information to a third party to enable a transaction without providing the account identifying information to the first party (i.e., note that the POS system does not get access to customers credit/debit account information, column 18, lines 5-47). Giorandano does not explicitly teach a time-varying code. In the same field of endeavor, Hsiao teaches a time varying multicharacter code, each time varying multicharacter code representing an identity of one of the respective entities (i.e., RPIN/SPIN, column 4, line 32-column 4, line 4). It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Hsiao within the system of Gioradano in order to enhance the security of the system.

Art Unit: 2435

As per claims 3 and 19, Gioradano further teaches the system wherein the multicharacter code is provided to the system via a secure electronic transmission device [column 18, lines 14-47].

As per claim 4 and 20, Gioradano further teaches the system wherein the code is encrypted and transmitted to the system and wherein the system is configured to decrypt the code with a public key of the entity [column 18, lines 14-47].

As per claims 5 and 21, Gioradano further teaches the system wherein said service provider's service includes delivery, wherein the information is an address to which an item is to be delivered to the entity, wherein the system receives the code and wherein the system uses the code to obtain the appropriate address for delivery of the item by the third party [column 18, lines 14-47].

As per claim 9-15, 41-45, 24-27, 30, 32 and 41-45 Gioradano further teaches the system wherein the account identifying information includes credit card information regarding the entity and the processor is configured to provide the credit card information based upon the code of the entity to enable the transaction [column 18, lines 14-47].

As per claims 28-29 and 33-39, Gioradano further teaches the system wherein the database is further configured to associate biometric information with each entity having secure data in the secure registry respectively [column 18, lines 14-47].

Art Unit: 2435

As per claim 46, Giordano further teaches the system wherein the identity of the entity is unknown until the code is mapped to the identity by the processor [column 18, lines 5-47].

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BEEMNET DADA whose telephone number is (571)272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BEEMNET DADA/
Primary Examiner, Art Unit 2435

Notice of References Cited	Application/Control No. 11/768,729	Applicant(s)/Patent Under Reexamination WEISS, KENNETH P.	
	Examiner BEEMNET DADA	Art Unit 2435	Page 1 of 1

U.S. PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A US-5,971,272	10-1999	Hsiao, Alaric S.	235/380
	B US-			
	C US-			
	D US-			
	E US-			
	F US-			
	G US-			
	H US-			
	I US-			
	J US-			
	K US-			
	L US-			
	M US-			


FOREIGN PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N				
	O				
	P				
	Q				
	R				
	S				
	T				

NON-PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)				
	U				
	V				
	W				
	X				

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes 	Application/Control No. 11768729	Applicant(s)/Patent Under Reexamination WEISS, KENNETH P.
	Examiner BEEMNET W DADA	Art Unit 2435

SEARCHED			
Class	Subclass	Date	Examiner
713	169, 182, 184	2/23/2012	BD
707	9	2/23/2012	BD

SEARCH NOTES		
Search Notes	Date	Examiner
East search	2/23/2012	BD
NPL search	2/23/2012	BD
Inventor name search	2/23/2012	BD

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

--	--

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with 37 CFR § 1.6(a)(4).

Dated: September 6, 2012
Electronic Signature for Matthew H. Grady: /Matthew H. Grady/

Docket No.: W0537-700620
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Kenneth P. Weiss

Application No.: 11/768,729

Confirmation No.: 3536

Filed: June 26, 2007

Art Unit: 2435

For: UNIVERSAL SECURE REGISTRY

Examiner: B. W. Dada

AMENDMENT IN RESPONSE TO NON-FINAL OFFICE ACTION UNDER 37 C.F.R. 1.111

Commissioner for Patents
Alexandria, VA 22313-1450

Dear Madam:

INTRODUCTORY COMMENTS

In response to the Office Action dated March 6, 2012, please amend the above-identified U.S. patent application as follows:

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 10 of this paper.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A secure registry system for providing information to a first party to enable transactions between the first party and entities with secure data stored in the secure registry system, the secure registry system comprising:
 - a database including secure data for each entity, wherein each entity is associated with a time-varying multicharacter code for each entity having secure data in the secure registry system, respectively, each time-varying multicharacter code representing an identity of one of the respective entities; and
 - a processor configured to receive, from the first party, at least the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed, configured to map the time-varying multicharacter code to the identity of the entity in the database using only the time-varying multicharacter code, and to access secure data associated with the entity including information required to enable the transaction, the information including account identifying information where the account identifying information is unknown to the first party, to provide the account identifying information to a third party to enable the transaction without providing the account identifying information to the first party.
2. (Canceled)
3. (Previously Presented) The system of claim 1, wherein the time-varying multicharacter code is provided to the system via a secure electronic transmission device.
4. (Previously Presented) The system of claim 1, wherein the time-varying multicharacter code is encrypted and transmitted to the system, and

wherein the system is configured to decrypt the time-varying multicharacter code with a public key of the entity.

5. (Previously Presented) The system as claimed in claim 1, wherein the transaction includes a service provided by the first party,

wherein said first party's service includes delivery,

wherein the information is an address to which an item is to be delivered to the entity,

wherein the system receives the time-varying multicharacter code, and

wherein the system uses the time-varying multicharacter code to obtain the appropriate address for delivery of the item by the third party.

6. – 8. (Cancelled)

9. (Currently Amended) The ~~secure registry~~ system as claimed in claim 1, wherein the account identifying information includes credit card account information regarding the entity, and wherein the processor is configured to provide the credit card account information based upon the multicharacter code of the entity to enable the transaction.

10. (Previously Presented) The system as claimed in claim 9, wherein the system is configured to receive an approval of the credit card transaction.

11. (Previously Presented) The system as claimed in claim 1, wherein the account identifying information includes bank card account information regarding the entity, and wherein the processor is configured to provide the bank card account information to enable the transaction based upon the multicharacter code of the entity.

12. (Previously Presented) The system as claimed in claim 11, wherein the system is configured to provide an approval of the bank card transaction.

13. (Previously Presented) The system as claimed in claim 1, wherein the information includes personal identification information regarding the entity.

14. (Previously Presented) The system as claimed in claim 13, wherein the personal identification information comprises a photograph of the entity, and wherein the photograph is provided to the first party.

15. (Previously Presented) The system as claimed in claim 1, wherein the account identifying information identifies email address information regarding the entity.

16. (Currently Amended) A method for providing information to a first party to enable transactions between the first party and entities who have secure data stored in a secure registry in which each entity is identified by a time-varying multicharacter code, the method comprising:

receiving the time-varying multicharacter code for an entity on whose behalf a transaction is to take place;

mapping the time-varying multicharacter code to an identity of the entity in a database using only the time-varying multicharacter code;

accessing information required to perform the transaction, the information including account identifying information unknown to the first party;

providing the account identifying information to a third party without providing the account identifying information to the first party; and

using the account identifying information to enable the first party to perform the transaction without the first party's knowledge of the account identifying information.

17. – 18. (Cancelled)

19. (Previously Presented) The method of claim 16, wherein the act of receiving the time-varying multicharacter code comprises receiving the time-varying multicharacter code transmitted via a secure electronic transmission device.

20. (Previously Presented) The method of claim 16, wherein the act of receiving the time-varying multicharacter code comprises receiving an encrypted multicharacter code, and wherein the method further comprises decrypting the encrypted multicharacter code.

21. (Previously Presented) The method as claimed in claim 16, wherein the transaction includes a service provided by the first party, wherein the service includes delivery, wherein the account identifying information is associated with an address to which an item is to be delivered for the entity, and wherein the third party receives the address for delivery of an item provided by the first party.

22. – 23. (Cancelled)

24. (Previously Presented) The method as claimed in claim 16, wherein the account identifying information includes a credit card number, and wherein the act of using the account identifying information comprises using the credit card number to enable the transaction.

25. (Previously Presented) The method as claimed in claim 24, wherein the act of using the account identifying information comprises receiving a validation or denial of the transaction without providing the credit card number of the entity to the first party.

26. (Previously Presented) The method as claimed in claim 16, wherein the act of using the account identifying information comprises using bank card information about the entity to enable a transaction.

27. (Previously Presented) The method as claimed in claim 26, wherein the act of using the information comprises receiving a validation or denial of the bank card transaction without providing a bank card number of the entity to the first party.

28. (Previously Presented) The method as claimed in claim 16, wherein the act of mapping the time-varying multicharacter code to information required by the first party comprises mapping the time-varying multicharacter code to personal identification information about the entity.

29. (Previously Presented) The method as claimed in claim 28, wherein the personal identification information comprises a photograph of the entity, and wherein the method further comprises an act of providing the photograph to the first party.

30. (Previously Presented) The method as claimed in claim 16, wherein the account identifying information identifies email address information about the entity.

31. (Canceled).

32. (Previously Presented) The method as claimed in claim 24, further comprising an act of transmitting to the first party one of an approval or a denial of the credit card transaction.

33. (Previously Presented) The system of claim 1, wherein the database is further configured to associate biometric information with each entity having secure data in the secure registry, respectively.

34. (Previously Presented) The system of claim 33, wherein the processor is further configured to map the time-varying multicharacter code to biometric information associated with the entity on whose behalf the transaction is to be performed and to provide the biometric information to the first party.

35. (Previously Presented) The system of claim 34, wherein the biometric information includes an image of the entity on whose behalf the transaction is to be performed.
36. (Previously Presented) The system of claim 34, wherein the time-varying multicharacter code is generated by a device associated with the entity on whose behalf the transaction is to be performed.
37. (Previously Presented) The method as claimed in claim 16, further comprising an act of associating biometric information with each entity having secure data in the secure registry, respectively.
38. (Previously Presented) The method of claim 37, further comprising acts of:
mapping the time-varying multicharacter code to biometric information associated with the entity on whose behalf the transaction is to be performed; and
providing the biometric information to the first party.
39. (Previously Presented) The method of claim 38, wherein the biometric information includes an image of the entity on whose behalf the transaction is to be performed.
40. (Canceled).
41. (Currently Amended) The ~~secure registry~~ system of claim 1, wherein the account identifying information includes an account number.
42. (Currently Amended) The ~~secure registry~~ system of claim 41, wherein the account identifying information includes credit card account information and the account number includes a credit card number.

43. (Currently Amended) The ~~secure registry~~ system of claim 41, wherein the third party includes a financial service provider and the account number includes at least one of a debit card number and a credit card number.
44. (Currently Amended) The ~~secure registry~~ of claim 43, wherein the first party includes a merchant, and the service includes a sale of at least one of goods and services.
45. (Currently Amended) The ~~secure registry~~ system of claim 44, wherein the processor is further configured to receive, from the first party, a merchant ID, and a purchase amount.
46. (Currently Amended) The ~~secure registry~~ system of claim 1, wherein the identity of the entity is unknown until the time-varying code is mapped to the identity by the processor.
47. (New) A secure registry system for providing information to a first party to enable transactions between the first party and entities with secure data stored in the secure registry system, the secure registry system comprising:
- a database including secure data for each entity, wherein each entity is associated with a time-varying multicharacter code for each entity having secure data in the secure registry system, respectively, each time-varying multicharacter code representing an identity of one of the respective entities, wherein the database is configured to permit or deny access to information on the respective entity using the time-varying multicharacter code; and
 - a processor configured to receive, the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed, configured to map the time-varying multicharacter code to the identity of the entity to identify the entity, configured to obtain from the database the secure data associated with the entity including information required to enable the transaction, the information including account identifying information, and configured to provide the account identifying information to a third party to enable the transaction without providing the account identifying information to the first party.

48. (New) A secure registry system for providing information to a first party to enable transactions between the first party and entities with secure data stored in the secure registry system, the secure registry system comprising:

a database including secure data for each entity, wherein each entity is associated with a time-varying multicharacter code for each entity having secure data in the secure registry system, respectively, each time-varying multicharacter code representing an identity of one of the respective entities; and

a processor configured to receive the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed, configured to map the time-varying multicharacter code to the identity of the entity without requiring further information to identify the entity, configured to access from the database secure data associated with the entity including information required to enable the transaction, the information including account identifying information, and configured to provide the account identifying information to a third party to enable the transaction without providing the account identifying information to the first party.

REMARKS

Claim 1, 3-5, 9-16, 19-21, 24-30, 32-39 and 41-46 were previously pending for examination with claims 1 and 16 being independent claims. Claims 47 and 48 have been added. Claims 1, 9, 16, and 41-46 have been amended. As a result claims 1, 3-5, 9-16, 19-21, 24-30, 32-39 and 41-48 are pending for examination with claims 1, 16, 47, and 48 being independent claims. No new matter has been added.

Examiner Interview

Applicant wishes to thank Examiner Dada for the courtesies extended to Applicant's Representative during the course of the Interview conducted on August 30, 2012. Applicant's Representative and Examiner Dada discussed the application and claims in light of the current rejection and the references of record. In particular, Applicant's Representative alleged that Hsiao does not teach or suggest a "time-varying multicharacter code for each entity having secure data in the secure registry system, respectively, each time-varying multicharacter code representing an identity of one of the respective entities," as recited in claim 1, for example. Applicant's Representative argued that Hsiao explicitly discloses identifying users with entry of respective account numbers (See e.g., Abstract, Col. 4, lines 6-11, and Col. 6, lines 1-5, lines 38-41, and lines 52-54) and, as disclosed in Hsiao, the RPIN/SPIN is used to validate the identified user (see e.g., Col. 4 line 32 – Col. 5, line 4).

Although agreement was not reached, Examiner Dada indicated that there are differences between the claimed approach and the disclosure in the references cited in the Office Action. Applicant's Representative and Examiner Dada discussed potential amendments to clarify the distinction over the current rejection. Accordingly, Applicant presents the current amendments and remarks, and respectfully requests reconsideration.

Rejections Under 35 U.S.C. §103

The Office Action rejected claims 1, 3-5, 9-16, 19-21, 24-30, 32-39 and 41-46 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 7,571,139 to Gioradano et al. (hereinafter *Gioradano*) in view of U.S. Patent No. 5,971,272 to Hsiao (hereinafter *Hsiao*).

Applicant respectfully asserts that that claims as amended herein are patentable in view of the cited references at least because Giordano and Hsiao alone or in proper combination do not teach or suggest a processor “configured to map the time-varying multicharacter code to the identity of the entity in the database using only the time-varying multicharacter code,” as recited in claim 1, as amended.

The Examiner admits and Applicant agrees that “Giordano does not explicitly teach a time-varying code.” (Office Action at page 3.) Instead, the Office Action relies on Hsiao for an alleged teaching of “a time-varying multicharacter code, each time-varying multicharacter code representing an identity of one of the respective entities (i.e., RPIN/SPIN, column 4, lines 32-column 4, line 4).” *Id.* Applicant respectfully notes that Hsiao does not cure the deficiencies of Giordano because, in Hsiao, the user necessarily also provides a static identification for an entity in the form of an account number: “verifying that a user has entered a *valid account identifier* as a preliminary condition to the account access provides additional security and avoids wasting resources which might otherwise be expended generating an RPIN for a non-existent account.” (Col. 7, lines 25-29; see also Abstract – “the present invention is readily applicable to any type of account which is accessed by *entry of an account number ...*”; and Col. 6, lines 52-54 - “the user responds to the request *by providing an appropriate account identifier*”).

According to Hsiao, a security mechanism is provided for conventional PINs, making them not “susceptible to detection by observation or repeated trial attempts.” (Col 3, lines 54-57). However, as discussed above, Hsiao teaches and relies on entry of account numbers prior to validating any RPIN/SPIN. Thus, Hsiao does not teach or suggest a processor “configured to map the time-varying multicharacter code to the identity of the entity in the database using only the time-varying multicharacter code,” as recited in claim 1, as amended.

As neither Giordano nor Hsiao teach or suggest this element, the combination, even if assumed proper does not teach or suggest claim 1. Claims 3-5, 9-15, 33-36, and 41-46 depend from claim 1 and are allowable for at least the same reasons. Accordingly, withdrawal of the rejection of claims 1, 3-5, 9-15, 33-36, and 41-46 is respectfully requested.

Likewise, the combination, even if assumed, proper does not teach or suggest “mapping the time-varying multicharacter code to an identity of the entity in a database using only the time-varying multicharacter code,” as recited in claim 16, amended. As admitted and agreed, Giordano does not teach or suggest a time-varying multicharacter code. Hsiao does not cure this deficiency, because, Hsiao does not teach or suggest “mapping the time-varying multicharacter code to an identity of the entity in a database using only the time-varying multicharacter code,” as recited in claim 16, amended. Rather, Hsiao teaches and relies on the use of a static account number to establish identity and then authorization using the RPIN/SPIN. Each RPIN/SPIN is associated with a specific account. (See e.g., Col. 4, lines 6-11). The account ***must be entered*** to access an retrieve PIN information, and only after accessing the account information can Hsiao validate a RPIN/SPIN. (Please see e.g., Col. 6, lines 1-5, lines 38-41, and lines 52-54). As neither reference, taken alone or in combination, teaches or suggests “mapping the time-varying multicharacter code to an identity of the entity in a database using only the time-varying multicharacter code,” the combination, even if assumed proper, does not teach or suggest claim 16, as amended.

Claims 19-21, 24-30, 32 and 37-39 depend from claim 16 and are allowable for at least the same reasons. Accordingly, withdrawal of the rejection of claims 16, 19-21, 24-30, 32 and 37-39 is respectfully requested.

New independent claim 47, is also patentable in view of the cited references at least because Giordano and Hsiao alone or in proper combination do not teach or suggest a database “configured to permit or deny access to information on the respective entity using the time-varying multicharacter code to obtain the information on the respective one of the entities,” and a processor “configured to map the time-varying multicharacter code to the identity of the entity” as recited in claim 47. As discussed, Giordano does not teach a time-varying multicharacter code, and Hsiao does not teach or suggest “using the time-varying multicharacter code to obtain the information on the respective one of the entities,” or a processor “configured to map the time-varying multicharacter code to the identity of the entity.” Rather, according to Hsiao, a static account number is used to obtain information. (Please see e.g., Col. 6, lines 1-5, lines 38-41, and lines 52-54). As neither reference, taken alone or in combination, teaches or suggests a database “configured to permit access to information on the respective entity using the time-varying multicharacter code

to obtain the information on the respective one of the entities,” as recited in claim 47, the combination, even if assumed proper, does not teach or suggest the claim.

Further, new independent claim 48 recites: a processor “configured to map the time-varying multicharacter code to the identity of the entity without requiring further information to identify the entity.” The alleged combination of Giordano and Hsiao, also does not teach or suggest this element, as Giordano does not teach a multicharacter code, and in Hsiao does not employ its RPIN/SPIN “to map” “to the identity of the entity without requiring further information to identify the entity,” as recited in the claim. Rather, according to Hsiao a static account number is used to identify an entity and then a submitted secure PIN is verified against information obtained using the static account number. (Please see e.g., Col. 6, lines 1-5, lines 38-41, and lines 52-54).

Accordingly, new claims 47-48 are also patentable in view of the cited references at least because Giordano and Hsiao alone or in proper combination do not teach or suggest at least one element of the respective independent claims.

CONCLUSION

In view of the foregoing amendments and remarks, reconsideration is respectfully requested. This application should now be in condition for allowance; a notice to this effect is respectfully requested. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicant's attorney at the telephone number listed below.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee that is not covered by an accompanying payment, please charge any deficiency to Deposit Account No. 50/2762.

Dated: September 6, 2012

Respectfully submitted,

Electronic signature: /Matthew H. Grady/

Matthew H. Grady

Registration No.: 52,957

John N. Anastasi

Registration No.: 37,765

LANDO & ANASTASI LLP

Riverfront Office Park

One Main Street

Suite 1100

Cambridge, Massachusetts 02142

(617) 395-7000

Attorney for Applicant

Electronic Patent Application Fee Transmittal

Application Number:	11768729
Filing Date:	26-Jun-2007
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Filer:	Matthew H. Grady
Attorney Docket Number:	W0537-7006

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Claims in excess of 20	2202	1	30	30
Independent claims in excess of 3	2201	1	125	125

Miscellaneous-Filing:

Petition:

Patent-Appeals-and-Interference:

Post-Allowance-and-Post-Issuance:

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Extension - 3 months with \$0 paid	2253	1	635	635
Miscellaneous:				
Total in USD (\$)				790

Electronic Acknowledgement Receipt

EFS ID:	13674258
Application Number:	11768729
International Application Number:	
Confirmation Number:	3536
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Correspondence Address:	John N. Anastasi c/o Lowrie, Lando & Anastasi, LLP Riverfront Office Park, One Main Street - Cambridge MA 02142 US 6173957000 -
Filer:	Matthew H. Grady
Filer Authorized By:	
Attorney Docket Number:	W0537-7006
Receipt Date:	06-SEP-2012
Filing Date:	26-JUN-2007
Time Stamp:	16:07:13
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$790

RAM confirmation Number	3225
Deposit Account	502762
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Amendment/Req. Reconsideration-After Non-Final Reject	W0537-700620_- _W0537-700620-NFOA_Rsp_1. pdf	60572 493dfc7a8452d455b79a0a385e3e472d0959131c	no	14

Warnings:

Information:

2	Fee Worksheet (SB06)	fee-info.pdf	33550 a40ac149ddda464b99b0594f857ea1bfc9c5ee47	no	2
---	----------------------	--------------	---	----	---

Warnings:

Information:

Total Files Size (in bytes):			94122
-------------------------------------	--	--	-------

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 11/768,729	Filing Date 06/26/2007	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

APPLICATION AS FILED – PART I			OTHER THAN SMALL ENTITY			
	(Column 1)	(Column 2)	SMALL ENTITY <input checked="" type="checkbox"/>	OR		
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	RATE (\$)	FEE (\$)
<input type="checkbox"/> BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>	N/A	N/A	N/A		N/A	
<input type="checkbox"/> SEARCH FEE <small>(37 CFR 1.16(k), (j), or (m))</small>	N/A	N/A	N/A		N/A	
<input type="checkbox"/> EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A	N/A		N/A	
TOTAL CLAIMS <small>(37 CFR 1.16(j))</small>	minus 20 =	*	X \$ =	OR	X \$ =	
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>	minus 3 =	*	X \$ =		X \$ =	
<input type="checkbox"/> APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).					
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.16(j))</small>						
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL		TOTAL	

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY			
	(Column 1)	(Column 2)	(Column 3)					
AMENDMENT	09/06/2012	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	* 38	Minus ** 37	= 1	X \$30 =	30	OR	X \$ =
	Independent <small>(37 CFR 1.16(h))</small>	* 4	Minus ***3	= 1	X \$125 =	125	OR	X \$ =
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>						OR	
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>						OR	
					TOTAL ADD'L FEE	155	OR	TOTAL ADD'L FEE

	(Column 1)	(Column 2)	(Column 3)					
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	*	Minus **	=	X \$ =		OR	X \$ =
	Independent <small>(37 CFR 1.16(h))</small>	*	Minus ***	=	X \$ =		OR	X \$ =
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>						OR	
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>						OR	
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
 ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
 *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
 The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/SHARAIN MORELAND/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
11/768,729 06/26/2007 Kenneth P. Weiss W0537-7006 3536

7590 12/18/2012
John N. Anastasi
c/o Lowrie, Lando & Anastasi, LLP
Riverfront Office Park, One Main Street
Cambridge, MA 02142

EXAMINER

DADA, BEEMNET W

ART UNIT PAPER NUMBER

2435

MAIL DATE DELIVERY MODE

12/18/2012

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

DETAILED ACTION

This office action is in reply to an amendment filed on September 06, 2012. Claims 1, 9, 16 and 41-46 have been amended and new claims 47 and 48 have been added. Claims 1, 3-5, 9-16, 19-21, 24-30, 32-39 and 41-48 are pending.

Response to Arguments

Applicant's arguments filed 09/06/2012 have been considered but are moot in view of new ground of rejection.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

Claims 1, 3-5, 9-16, 19-21, 24-30, 32-39 and 41-48 are rejected under 35 U.S.C. 103(a) as being unpatentable over Gioradano et al. US 7,571,139 B1 (hereinafter Gioradano) in view Weiss US 5,657,388.

As per claims 1, 16, 47 and 48, Giorandano teaches a secure registry system for providing information to a service provider to enable the service provider to provide services to entities with secure data stored in the secure registry system, comprising:

Art Unit: 2435

a database including secure data for each entity, wherein each entity is associated with and a multicharacter_code for each entity having secure data in the secure registry system, respectively [column 18, lines 14-47] and

a processor configured to receive, from the first party, the multicharacter code for the entity on whose behalf of a transaction is to be performed, configured to map the multicharacter code to the identity of the entity and secure data associated with the entity including information required to enable the transaction, the information including account identifying information where the account identifying information is unknown to the first party, to provide the account identifying information to a third party to enable a transaction without providing the account identifying information to the first party (i.e., note that the POS system does not get access to customers credit/debit account information, column 18, lines 5-47). Giorandano does not explicitly teach a time-varying code. In the same field of endeavor, Weiss teaches a time varying multi character code, mapping the time-varying multi character code to the identity of an entity in a database using only the time-varying multi character code (i.e., one time non predictable code). It would have been obvious to one having ordinary skill in the art at the time of applicant's invention to employ the teachings of Weiss within the system of Gioradano in order to enhance the security of the system.

As per claims 3 and 19, Gioradano further teaches the system wherein the multicharacter code is provided to the system via a secure electronic transmission device [column 18, lines 14-47].

As per claim 4 and 20, Gioradano further teaches the system wherein the code is encrypted and transmitted to the system and wherein the system is configured to decrypt the code with a public key of the entity [column 18, lines 14-47].

As per claims 5 and 21, Gioradano further teaches the system wherein said service provider's service includes delivery, wherein the information is an address to which an item is to be delivered to the entity, wherein the system receives the code and wherein the system uses the code to obtain the appropriate address for delivery of the item by the third party [column 18, lines 14-47].

As per claim 9-15, 41-45, 24-27, 30, 32 and 41-45 Gioradano further teaches the system wherein the account identifying information includes credit card information regarding the entity and the processor is configured to provide the credit card information based upon the code of the entity to enable the transaction [column 18, lines 14-47].

As per claims 28-29 and 33-39, Gioradano further teaches the system wherein the database is further configured to associate biometric information with each entity having secure data in the secure registry respectively [column 18, lines 14-47].

As per claim 46, Giordano further teaches the system wherein the identity of the entity is unknown until the code is mapped to the identity by the processor [column 18, lines 5-47].

Conclusion

Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire **THREE MONTHS** from the mailing date of this action. In the event a first reply is filed within **TWO MONTHS** of the mailing date of this final action and the advisory action is not mailed until after the end of the **THREE-MONTH** shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than **SIX MONTHS** from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to BEEMNET DADA whose telephone number is (571)272-3847. The examiner can normally be reached on Monday - Friday (9:00 am - 5:30 pm).

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2435

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/BEEMNET DADA/
Primary Examiner, Art Unit 2435

Notice of References Cited	Application/Control No. 11/768,729	Applicant(s)/Patent Under Reexamination WEISS, KENNETH P.	
	Examiner BEEMNET DADA	Art Unit 2435	Page 1 of 1

U.S. PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A US-5,657,388	08-1997	Weiss, Kenneth P.	713/185
	B US-			
	C US-			
	D US-			
	E US-			
	F US-			
	G US-			
	H US-			
	I US-			
	J US-			
	K US-			
	L US-			
	M US-			


FOREIGN PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N				
	O				
	P				
	Q				
	R				
	S				
	T				

NON-PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)				
	U				
	V				
	W				
	X				

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes 	Application/Control No. 11768729	Applicant(s)/Patent Under Reexamination WEISS, KENNETH P.
	Examiner BEEMNET W DADA	Art Unit 2435

SEARCHED			
Class	Subclass	Date	Examiner
713	169, 182, 184	12/10/2012	BD
707	9	12/10/2012	BD

SEARCH NOTES		
Search Notes	Date	Examiner
East search	12/10/2012	BD
NPL search	12/10/2012	BD
Inventor name search	12/10/2012	BD

INTERFERENCE SEARCH			
Class	Subclass	Date	Examiner

--	--

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

CHANGE OF CORRESPONDENCE ADDRESS Application	Application Number	11/768,729
	Filing Date	June 26, 2007
	First Named Inventor	Kenneth P. Weiss
	Art Unit	2435
	Examiner Name	B. W. Dada
	Attorney Docket No.	W0537-700620
Address to: Commissioner for Patents P.O. Box 1450 Alexandria, VA 22313-1450		

Please change the Correspondence Address for the above-identified application to:

The address associated with Customer Number:

OR

<input type="checkbox"/> Firm or Individual Name				
Address				
City		State		Zip
Country				
Telephone		Email		

This form cannot be used to change the data associated with a Customer Number. To change the data associated with an existing Customer Number use "Request for Customer Number Data Change" (PTO/SB/124).

I am the:

Applicant/Inventor

Assignee of record of the entire interest.
Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).

Attorney or agent of record. Registration Number 52,957.

Registered practitioner named in the application transmittal letter in an application without an executed oath or declaration. See 37 CFR 1.33(a)(1). Registration Number _____.

Signature /Matthew H. Grady/

Typed or Printed Name Matthew H. Grady

Date January 25, 2013 Telephone (617) 395-7017

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

*Total of 1 forms are submitted.

1507522.1

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with 37 CFR § 1.6(a)(4).	
Dated: January 25, 2013	Electronic Signature for Matthew H. Grady: <u>/Matthew H. Grady/</u>

1507522

0676

Electronic Acknowledgement Receipt

EFS ID:	14789024
Application Number:	11768729
International Application Number:	
Confirmation Number:	3536
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Correspondence Address:	John N. Anastasi c/o Lowrie, Lando & Anastasi, LLP Riverfront Office Park, One Main Street - Cambridge MA 02142 US 6173957000 -
Filer:	Matthew H. Grady
Filer Authorized By:	
Attorney Docket Number:	W0537-7006
Receipt Date:	25-JAN-2013
Filing Date:	26-JUN-2007
Time Stamp:	10:10:48
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Change of Address	W0537-700620_- _Change_of_Correspondence_ Address_-- _Application_PTO_SB-122_1. PDF	21410 5a1529df3d551ca02a52652d4d2d12b47bef106d0	no	1

Warnings:

Information:

Total Files Size (in bytes):	21410
-------------------------------------	-------

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with 37 CFR § 1.6(a)(4).

Dated: April 12, 2013
Electronic Signature for Matthew H. Grady: /Matthew H. Grady/

Docket No.: W0537-700620
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Kenneth P. Weiss

Application No.: 11/768,729

Confirmation No.: 3536

Filed: June 26, 2007

Art Unit: 2435

For: UNIVERSAL SECURE REGISTRY

Examiner: B. W. Dada

AMENDMENT AFTER FINAL ACTION UNDER 37 C.F.R. 1.116

Commissioner for Patents

Dear Madam:

INTRODUCTORY COMMENTS

In response to the Office Action mailed on December 18, 2012, please amend the above-identified application as follows: Changes to the claims are shown by strike through (for deleted matter) and underlining (for added matter).

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 10 of this paper.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A secure registry system for providing information to a first party to enable transactions between the first party and entities with secure data stored in the secure registry system, the secure registry system comprising:

a database including secure data for each entity, wherein each entity is associated with a time-varying multicharacter code for each entity having secure data in the secure registry system, respectively, each time-varying multicharacter code representing an identity of one of the respective entities; and

a processor configured to receive, from the first party, at least the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed, configured to map the time-varying multicharacter code to the identity of the entity in the database using only the time-varying multicharacter code, to execute a restriction mechanism configured to determine compliance with any access restrictions for the first party, and to access secure data associated with the entity including information required to enable the transaction, the information including account identifying information where the account identifying information is unknown to the first party, to provide the account identifying information to a third party to enable the transaction without providing the account identifying information to the first party.

2. (Canceled)

3. (Previously Presented) The system of claim 1, wherein the time-varying multicharacter code is provided to the system via a secure electronic transmission device.

4. (Previously Presented) The system of claim 1, wherein the time-varying multicharacter code is encrypted and transmitted to the system, and

wherein the system is configured to decrypt the time-varying multicharacter code with a public key of the entity.

5. (Previously Presented) The system as claimed in claim 1, wherein the transaction includes a service provided by the first party,
wherein said first party's service includes delivery,
wherein the information is an address to which an item is to be delivered to the entity,
wherein the system receives the time-varying multicharacter code, and
wherein the system uses the time-varying multicharacter code to obtain the appropriate address for delivery of the item by the third party.
6. (Canceled)
7. (Canceled)
8. (Canceled)
9. (Previously Presented) The system as claimed in claim 1, wherein the account identifying information includes credit card account information regarding the entity, and wherein the processor is configured to provide the credit card account information based upon the multicharacter code of the entity to enable the transaction.
10. (Previously Presented) The system as claimed in claim 9, wherein the system is configured to receive an approval of the credit card transaction.
11. (Previously Presented) The system as claimed in claim 1, wherein the account identifying information includes bank card account information regarding the entity, and wherein the processor is configured to provide the bank card account information to enable the transaction based upon the multicharacter code of the entity.
12. (Previously Presented) The system as claimed in claim 11, wherein the system is configured to provide an approval of the bank card transaction.

13. (Previously Presented) The system as claimed in claim 1, wherein the information includes personal identification information regarding the entity.

14. (Previously Presented) The system as claimed in claim 13, wherein the personal identification information comprises a photograph of the entity, and wherein the photograph is provided to the first party.

15. (Previously Presented) The system as claimed in claim 1, wherein the account identifying information identifies email address information regarding the entity.

16. (Previously Presented) A method for providing information to a first party to enable transactions between the first party and entities who have secure data stored in a secure registry in which each entity is identified by a time-varying multicharacter code, the method comprising:

receiving the time-varying multicharacter code for an entity on whose behalf a transaction is to take place;

mapping the time-varying multicharacter code to an identity of the entity in a database using only the time-varying multicharacter code;

determining compliance based on any access restrictions for the first party;

accessing information required to perform the transaction, the information including account identifying information unknown to the first party;

providing the account identifying information to a third party without providing the account identifying information to the first party; and

using the account identifying information to enable the first party to perform the transaction without the first party's knowledge of the account identifying information.

17. (Canceled)

18. (Canceled)

19. (Previously Presented) The method of claim 16, wherein the act of receiving the time-varying multicharacter code comprises receiving the time-varying multicharacter code transmitted via a secure electronic transmission device.

20. (Previously Presented) The method of claim 16, wherein the act of receiving the time-varying multicharacter code comprises receiving an encrypted multicharacter code, and wherein the method further comprises decrypting the encrypted multicharacter code.

21. (Previously Presented) The method as claimed in claim 16, wherein the transaction includes a service provided by the first party,
wherein the service includes delivery,
wherein the account identifying information is associated with an address to which an item is to be delivered for the entity, and
wherein the third party receives the address for delivery of an item provided by the first party.

22. (Canceled)

23. (Canceled)

24. (Previously Presented) The method as claimed in claim 16, wherein the account identifying information includes a credit card number, and wherein the act of using the account identifying information comprises using the credit card number to enable the transaction.

25. (Previously Presented) The method as claimed in claim 24, wherein the act of using the account identifying information comprises receiving a validation or denial of the transaction without providing the credit card number of the entity to the first party.

26. (Previously Presented) The method as claimed in claim 16, wherein the act of using the account identifying information comprises using bank card information about the entity to enable a transaction.

27. (Previously Presented) The method as claimed in claim 26, wherein the act of using the information comprises receiving a validation or denial of the bank card transaction without providing a bank card number of the entity to the first party.

28. (Previously Presented) The method as claimed in claim 16, wherein the act of mapping the time-varying multicharacter code to information required by the first party comprises mapping the time-varying multicharacter code to personal identification information about the entity.

29. (Previously Presented) The method as claimed in claim 28, wherein the personal identification information comprises a photograph of the entity, and
wherein the method further comprises an act of providing the photograph to the first party.

30. (Previously Presented) The method as claimed in claim 16, wherein the account identifying information identifies email address information about the entity.

31. (Canceled).

32. (Previously Presented) The method as claimed in claim 24, further comprising an act of transmitting to the first party one of an approval or a denial of the credit card transaction.

33. (Previously Presented) The system of claim 1, wherein the database is further configured to associate biometric information with each entity having secure data in the secure registry, respectively.

34. (Previously Presented) The system of claim 33, wherein the processor is further configured to map the time-varying multicharacter code to biometric information associated with the entity on whose behalf the transaction is to be performed and to provide the biometric information to the first party.

35. (Previously Presented) The system of claim 34, wherein the biometric information includes an image of the entity on whose behalf the transaction is to be performed.
36. (Previously Presented) The system of claim 34, wherein the time-varying multicharacter code is generated by a device associated with the entity on whose behalf the transaction is to be performed.
37. (Previously Presented) The method as claimed in claim 16, further comprising an act of associating biometric information with each entity having secure data in the secure registry, respectively.
38. (Previously Presented) The method of claim 37, further comprising acts of:
mapping the time-varying multicharacter code to biometric information associated with the entity on whose behalf the transaction is to be performed; and
providing the biometric information to the first party.
39. (Previously Presented) The method of claim 38, wherein the biometric information includes an image of the entity on whose behalf the transaction is to be performed.
40. (Canceled).
41. (Previously Presented) The system of claim 1, wherein the account identifying information includes an account number.
42. (Previously Presented) The system of claim 41, wherein the account identifying information includes credit card account information and the account number includes a credit card number.

43. (Previously Presented) The system of claim 41, wherein the third party includes a financial service provider and the account number includes at least one of a debit card number and a credit card number.

44. (Currently Amended) The system of claim 43, wherein the first party includes a merchant, and the service includes a sale of at least one of goods and services.

45. (Previously Presented) The system of claim 44, wherein the processor is further configured to receive, from the first party, a merchant ID, and a purchase amount.

46. (Previously Presented) The system of claim 1, wherein the identity of the entity is unknown until the time-varying code is mapped to the identity by the processor.

47. (Currently Amended) A secure registry system for providing information to a first party to enable transactions between the first party and entities with secure data stored in the secure registry system, the secure registry system comprising:

a database including secure data for each entity, wherein each entity is associated with a time-varying multicharacter code for each entity having secure data in the secure registry system, respectively, each time-varying multicharacter code representing an identity of one of the respective entities, wherein the database is configured to permit or deny access to information on the respective entity using the time-varying multicharacter code; and

a processor configured to receive, the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed, configured to map the time-varying multicharacter code to the identity of the entity to identify the entity, configured to execute a restriction mechanism configured to determine compliance with any access restrictions for the first party, configured to obtain from the database the secure data associated with the entity including information required to enable the transaction, the information including account identifying information, and configured to provide the account identifying information to a third party to enable the transaction without providing the account identifying information to the first party.

48. (Currently Amended) A secure registry system for providing information to a first party to enable transactions between the first party and entities with secure data stored in the secure registry system, the secure registry system comprising:

a database including secure data for each entity, wherein each entity is associated with a time-varying multicharacter code for each entity having secure data in the secure registry system, respectively, each time-varying multicharacter code representing an identity of one of the respective entities; and

a processor configured to receive the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed, configured to map the time-varying multicharacter code to the identity of the entity without requiring further information to identify the entity, configured to access from the database secure data associated with the entity including information required to enable the transaction, the information including account identifying information, and configured to provide the account identifying information to a third party to enable the transaction without providing the account identifying information to the first party, and wherein enabling the transaction without providing account identifying information to the first party includes limiting the account identifying information provided by the secure registry system to the first party to transaction approval information.

REMARKS

Claims 1, 3-5, 9-16, 19-21, 24-30, 32-39 and 41-48 were previously pending in this application. Claims 1, 16, 44, 47 and 48 have been amended. As a result claims 1, 3-5, 9-16, 19-21, 24-30, 32-39 and 41-48 are pending for examination with claims 1, 16, 47 and 48 being independent claims. No new matter has been added.

Examiner Interview

Applicant wishes to thank Examiner Dada for the courtesies extended to Applicant's Representative during the course of the Interview conducted on April 9, 2013. During the course of the Interview, the participants discussed the Application, Office Action, the rejections of record and proposed amendments. In particular, Applicant proposed amendment to claim 1. Claim 1, as amended, now recites "a restriction mechanism configured to determine compliance with any access restrictions for the first party," which is not taught or suggested by Giordano or Weiss. Although agreement as to the allowability of the claims was not reached, Examiner Dada agreed that the proposed amendments would overcome the present rejection. Accordingly, presented are the amendments to the claims discussed. Favorable consideration is respectfully requested.

Rejections Under 35 U.S.C. §103

The Office Action rejected claims 1, 3-5, 9-16, 19-21, 24-30, 32-39 and 41-48 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 7,571,139 B1 to Gioradano et al. (hereinafter Gioradano) in view of U.S. Patent No. 5,657,388 to Weiss (hereinafter Weiss). In response, Applicant has amended claims 1, 16, 47 and 48 and submits the following remarks.

Applicant respectfully asserts that the claim 1, as amended, is patentable in view of the alleged combination at least because Giordano and Weiss alone or in proper combination do not teach or suggest "a restriction mechanism configured to determine compliance with any access restrictions for the first party," as recited in claim 1, as amended.

Giordano is directed to "a network for processing retail sales transactions" including "a customer transceiver with a unique customer number" (Abstract). Giordano teaches a "transaction processing system" that processes transactions with the "appropriate payment processing center" based on received authorization requests including "the customer ID, merchant ID and transaction data" (Col. 3 Lines 29-36). In summary, Giordano teaches the use

of a customer transceiver to authorize a transaction processing system to carry out a monetary transaction between a customer and a merchant at the appropriate payment processing center.

Giordano does not teach or suggest “a restriction mechanism configured to determine compliance with any access restrictions for the first party,” as recited in claim 1, as amended. Rather, Giordano teaches the use of a customer transceiver to authorize a transaction processing system to carry out a monetary transaction between a customer and a merchant at the appropriate payment processing center. Accordingly, claim 1, as amended, distinguishes over the Giordano reference.

Weiss is directed to “a method and apparatus for utilizing a token” to “provide secure access by authorized users to a selected resource” (Abstract). Weiss teaches the generation and use of a one-time variable multi-character code based in part on information stored in the token to authenticate the user’s identity. Weiss does not teach or suggest “a restriction mechanism configured to determine compliance with any access restrictions for the first party,” as recited in claim 1, as amended. Rather, Weiss teaches the use of a one-time variable multi-character code based in part on information stored in a user’s token to authenticate a user. Accordingly, claim 1, as amended, distinguishes over the Weiss reference.

As neither Giordano nor Weiss teach or suggest this element, the combination, even if assumed proper, does not teach or suggest claim 1. Claims 3-5, 9-15, 33-36 and 41-46 depend from claim 1 and are allowable for at least the same reasons. Accordingly, withdrawal of the rejection of claims 1, 3-5, 9-15, 33-36 and 41-46 under 35 U.S.C. §103(a) is respectfully requested.

Independent Claim 16

Independent claim 16, as amended, recites “determining compliance based on any access restrictions for the first party.” As discussed above with respect to claim 1, Giordano teaches the use of a customer transceiver to authorize a transaction processing system to carry out a monetary transaction between a customer and a merchant at the appropriate payment processing center. Thus, Giordano does teach or suggest “determining compliance based on any access restrictions for the first party,” as recited in claim 16, as amended. Assuming the combination is proper, the addition of Weiss does not cure this deficiency as Weiss does not teach or suggest “determining compliance based on any access restrictions for the first party,” as recited in claim

16, as amended. Claims 19-21, 24-30, 32 and 37-39 depend from claim 16 and are allowable for at least the same reasons. Accordingly, withdrawal of the rejection of claims 16, 19-21, 24-30, 32 and 37-39 under 35 U.S.C. §103(a) is respectfully requested.

Independent Claim 47

Independent claim 47 is also patentable in view of the alleged combination at least because Giordano and Weiss alone or in proper combination do not teach or suggest “a restriction mechanism configured to determine compliance with any access restrictions for the first party,” as recited in claim 47, as amended. As discussed above with respect to claim 1, Giordano teaches the use of a customer transceiver to authorize a transaction processing system to carry out a monetary transaction between a customer and a merchant at the appropriate payment processing center. The addition of Weiss does not cure this deficiency. Accordingly, withdrawal of the rejection of claim 47 under 35 U.S.C. §103(a) is respectfully requested.

Independent Claim 48

Independent claim 48, as amended, is patentable in view of the alleged combination at least because Giordano and Weiss alone or in proper combination do not teach or suggest “wherein enabling the transaction without providing account identifying information to the first party includes limiting the account identifying information provided by the secure registry system to the first party to transaction approval information,” as recited claim 48, as amended. Giordano teaches the “transaction processing system” transmitting to the online merchant “identification information and other data unique to the associated customer in the absence of a retail transaction” (See Col. 4 Lines 17-21). Giordano explicitly teaches the transmission of information regarding the user (e.g., entity or purchaser), including loyalty program information (See e.g., Col. 4 Lines 54-58), to a merchant (e.g., first party) rather than limiting the information transmitted to the merchant to transaction approval information. Accordingly, Giordano does not teach or suggest claim 48, as amended. Assuming the combination is proper, the addition of Weiss does not cure this deficiency. Weiss teaches the use of a one-time variable multi-character code based in part on information stored in a user’s token to authenticate a user. Thus, Weiss does not teach “wherein enabling the transaction without providing account identifying information to the first party includes limiting the account identifying information

provided by the secure registry system to the first party to transaction approval information,” as recited in claim 48, as amended. Accordingly, withdrawal of the rejection of claim 48 under 35 U.S.C. §103(a) is respectfully requested.

CONCLUSION

In view of the foregoing amendments and remarks, reconsideration is respectfully requested. This application should now be in condition for allowance; a notice to this effect is respectfully requested. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicant's attorney at the telephone number listed below.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee that is not covered by an accompanying payment, please charge any deficiency to Deposit Account No. 50/2762 (W0537-700620).

Dated: April 12, 2013

Respectfully submitted,

Electronic signature: /Matthew H. Grady/
Matthew H. Grady

Registration No.: 52,957

John N. Anastasi

Registration No.: 37,765

LANDO & ANASTASI LLP

Riverfront Office Park
One Main Street
Suite 1100
Cambridge, Massachusetts 02142
(617) 395-7000

Attorney for Applicant

Electronic Patent Application Fee Transmittal

Application Number:	11768729
Filing Date:	26-Jun-2007
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Filer:	Matthew H. Grady
Attorney Docket Number:	W0537-700620

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 1 month with \$0 paid	2251	1	100	100

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				100

Electronic Acknowledgement Receipt

EFS ID:	15500134
Application Number:	11768729
International Application Number:	
Confirmation Number:	3536
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Customer Number:	37462
Filer:	Matthew H. Grady
Filer Authorized By:	
Attorney Docket Number:	W0537-700620
Receipt Date:	12-APR-2013
Filing Date:	26-JUN-2007
Time Stamp:	09:34:13
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$100
RAM confirmation Number	7667
Deposit Account	502762
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		1583451_1- Amendment_After_Final_Actio n_Under_37_CFR_1116_1.pdf	72559 9360286fb66d2e9bcb3e9cec644dbce21a9e01e	yes	13

Multipart Description/PDF files in .zip description

Document Description	Start	End
Amendment After Final	1	1
Claims	2	9
Applicant Arguments/Remarks Made in an Amendment	10	13

Warnings:

Information:

2	Fee Worksheet (SB06)	fee-info.pdf	30192 39994e2637acdeca787e021e647549031bf b86d4	no	2
---	----------------------	--------------	---	----	---

Warnings:

Information:

Total Files Size (in bytes): 102751

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 11/768,729	Filing Date 06/26/2007	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

APPLICATION AS FILED – PART I			OTHER THAN SMALL ENTITY			
	(Column 1)	(Column 2)	SMALL ENTITY <input checked="" type="checkbox"/>	OR		
FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)	RATE (\$)	FEE (\$)
<input type="checkbox"/> BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>	N/A	N/A	N/A		N/A	
<input type="checkbox"/> SEARCH FEE <small>(37 CFR 1.16(k), (j), or (m))</small>	N/A	N/A	N/A		N/A	
<input type="checkbox"/> EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A	N/A		N/A	
TOTAL CLAIMS <small>(37 CFR 1.16(j))</small>	minus 20 =	*	X \$ =	OR	X \$ =	
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>	minus 3 =	*	X \$ =		X \$ =	
<input type="checkbox"/> APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$250 (\$125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).					
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.16(j))</small>						
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL		TOTAL	

APPLICATION AS AMENDED – PART II					OTHER THAN SMALL ENTITY			
	(Column 1)	(Column 2)	(Column 3)					
AMENDMENT	04/12/2013	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	* 38	Minus ** 38	= 0	X \$40 =	0	OR	X \$ =
	Independent <small>(37 CFR 1.16(h))</small>	* 4	Minus ***4	= 0	X \$210 =	0	OR	X \$ =
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>						OR	
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>						OR	
					TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE

	(Column 1)	(Column 2)	(Column 3)					
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	RATE (\$)	ADDITIONAL FEE (\$)
	Total <small>(37 CFR 1.16(i))</small>	*	Minus **	=	X \$ =		OR	X \$ =
	Independent <small>(37 CFR 1.16(h))</small>	*	Minus ***	=	X \$ =		OR	X \$ =
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>						OR	
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>						OR	
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
 ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
 *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
 The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/BRENDA J. DENNY/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/768,729	06/26/2007	Kenneth P. Weiss	W0537-700620	3536
37462	7590	05/01/2013	EXAMINER	
LANDO & ANASTASI, LLP ONE MAIN STREET, SUITE 1100 CAMBRIDGE, MA 02142			DADA, BEEMNET W	
			ART UNIT	PAPER NUMBER
			2435	
			NOTIFICATION DATE	DELIVERY MODE
			05/01/2013	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@LALaw.com
gengelso@LALaw.com

Applicant-Initiated Interview Summary	Application No. 11/768,729	Applicant(s) WEISS, KENNETH P.	
	Examiner BEEMNET DADA	Art Unit 2435	

All participants (applicant, applicant's representative, PTO personnel):

- (1) BEEMNET DADA. (3)_____.
- (2) Matthew Grady. (4)_____.

Date of Interview: 09 April 2013.

Type: Telephonic Video Conference
 Personal [copy given to: applicant applicant's representative]

Exhibit shown or demonstration conducted: Yes No.
If Yes, brief description: _____.

Issues Discussed 101 112 102 103 Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: 1,16,47 and 48.

Identification of prior art discussed: Giordano and Weiss.

Substance of Interview

(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Applicant proposed amendment to the claims and indicated that the proposed amendment is not taught by the prior art on record. Examiner agreed the proposed amendment is not taught by the prior art on record but indicated further consideration is needed to determine allowability of the claims.

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

Attachment

/BEEMNET DADA/
Primary Examiner, Art Unit 2435

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record

A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews

Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.

All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:

- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:

- 1) A brief description of the nature of any exhibit shown or any demonstration conducted,
- 2) an identification of the claims discussed,
- 3) an identification of the specific prior art discussed,
- 4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
- 5) a brief identification of the general thrust of the principal arguments presented to the examiner,
(The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
- 6) a general indication of any other pertinent matters discussed, and
- 7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

Advisory Action Before the Filing of an Appeal Brief	Application No. 11/768,729	Applicant(s) WEISS, KENNETH P.
	Examiner BEEMNET DADA	Art Unit 2435

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 12 April 2013 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

NO NOTICE OF APPEAL FILED

1. The reply was filed after a final rejection. No Notice of Appeal has been filed. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114 if this is a utility or plant application. Note that RCEs are not permitted in design applications. The reply must be filed within one of the following time periods:

- a) The period for reply expires 4 months from the mailing date of the final rejection.
- b) The period for reply expires on: (1) the mailing date of this Advisory Action; or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.
- c) A prior Advisory Action was mailed more than 3 months after the mailing date of the final rejection in response to a first after-final reply filed within 2 months of the mailing date of the final rejection. The current period for reply expires _____ months from the mailing date of the prior Advisory Action or SIX MONTHS from the mailing date of the final rejection, whichever is earlier.

Examiner Note: If box 1 is checked, check either box (a), (b) or (c). ONLY CHECK BOX (b) WHEN THIS ADVISORY ACTION IS THE FIRST RESPONSE TO APPLICANT'S FIRST AFTER-FINAL REPLY WHICH WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. ONLY CHECK BOX (c) IN THE LIMITED SITUATION SET FORTH UNDER BOX (c). See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) or (c) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. The proposed amendments filed after a final rejection, but prior to the date of filing a brief, will not be entered because

- a) They raise new issues that would require further consideration and/or search (see NOTE below);
- b) They raise the issue of new matter (see NOTE below);
- c) They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
- d) They present additional claims without canceling a corresponding number of finally rejected claims.

NOTE: See Continuation Sheet. (See 37 CFR 1.116 and 41.33(a)).

4. The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).

5. Applicant's reply has overcome the following rejection(s): _____.

6. Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).

7. For purposes of appeal, the proposed amendment(s): (a) will not be entered, or (b) will be entered, and an explanation of how the new or amended claims would be rejected is provided below or appended.

AFFIDAVIT OR OTHER EVIDENCE

8. The affidavit or other evidence filed after final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).

9. The affidavit or other evidence filed after the date of filing the Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing of good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).

10. The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. The request for reconsideration has been considered but does NOT place the application in condition for allowance because:
See Continuation Sheet.

12. Note the attached Information Disclosure Statement(s). (PTO/SB/08) Paper No(s). _____

13. Other: Interview Summary 04/09/2013 attached.

STATUS OF CLAIMS

14. The status of the claim(s) is (or will be) as follows:

- Claim(s) allowed: _____
- Claim(s) objected to: _____
- Claim(s) rejected: 1,3-5,9-16,19-21,24-30,32-39 and 41-48.
- Claim(s) withdrawn from consideration: _____

/BEEMNET DADA/
Primary Examiner, Art Unit 2435

Continuation of 3. NOTE: New claim language would require further consideration.

Continuation of 11. does NOT place the application in condition for allowance because: Examiner would point out that, a search for the claims as amended indicates the claims are not in condition for allowance. See for example US Patent 6,018,724 for claims 1, 16 and 47 newly added limitations.

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with 37 CFR § 1.6(a)(4).

Dated: April 12, 2013
Electronic Signature for Matthew H. Grady: /Matthew H. Grady/

Docket No.: W0537-700620
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Kenneth P. Weiss

Application No.: 11/768,729

Confirmation No.: 3536

Filed: June 26, 2007

Art Unit: 2435

For: UNIVERSAL SECURE REGISTRY

Examiner: B. W. Dada

DO NOT ENTER: /BD/

AMENDMENT AFTER FINAL ACTION UNDER 37 C.F.R. 1.116

Commissioner for Patents

Dear Madam:

INTRODUCTORY COMMENTS

In response to the Office Action mailed on December 18, 2012, please amend the above-identified application as follows: Changes to the claims are shown by strike through (for deleted matter) and underlining (for added matter).

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 10 of this paper.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL (Submitted Only via EFS-Web)

Application Number	11768729	Filing Date	2007-06-26	Docket Number (if applicable)	W0537-700620	Art Unit	2435
First Named Inventor	Kenneth P. Weiss			Examiner Name	B. W. Dada		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

Other _____

Enclosed

Amendment/Reply

Information Disclosure Statement (IDS)

Affidavit(s)/ Declaration(s)

Other _____

MISCELLANEOUS

Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

Other _____

FEES

The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.

The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 50/2762

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Patent Practitioner Signature

Applicant Signature

Signature of Registered U.S. Patent Practitioner			
Signature	/Matthew H. Grady/	Date (YYYY-MM-DD)	2013-05-20
Name	Matthew H. Grady	Registration Number	52957

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with 37 CFR § 1.6(a)(4).

Dated: May 20, 2013
Electronic Signature for Matthew H. Grady: /Matthew H. Grady/

Docket No.: W0537-700620
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Kenneth P. Weiss

Application No.: 11/768,729

Confirmation No.: 3536

Filed: June 26, 2007

Art Unit: 2435

For: UNIVERSAL SECURE REGISTRY

Examiner: B. W. Dada

INFORMATION DISCLOSURE STATEMENT (IDS)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Madam:

Pursuant to 37 C.F.R. § 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the references listed on the attached PTO/SB/08. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the references be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

The applicant would like to bring to the Examiner's attention the following co-pending applications that may contain subject matter related to this application:

Serial No.	Filing Date	Inventor	Patent/Publication No.
13/621,609	17-Sep-2012	Kenneth P. Weiss	US 2013-0024374 A1
13/168,556	24-Jun-2011	Kenneth P. Weiss	8,271,397
13/237,184	20-Sep-2011	Kenneth P. Weiss	US 2012-0130904 A1
13/234,874	16-Sep-2011	Kenneth P. Weiss	US 2012-0240195 A1

In accordance with 37 C.F.R. § 1.97(g), the filing of this Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 C.F.R. § 1.56(a) exists. In accordance with 37 C.F.R. § 1.97(h), the filing of this Information Disclosure Statement shall not be construed to be an admission that any patent, publication or other information referred to therein is “prior art” for this invention unless specifically designated as such.

It is submitted that the Information Disclosure Statement is in compliance with 37 C.F.R. § 1.98 and the Examiner is respectfully requested to consider the listed references.

The Director is hereby authorized to charge any deficiency in the fees filed, asserted to be filed or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to our Deposit Account No. 50/2762, under Order No. W0537-700620.

Dated: May 20, 2013

Respectfully submitted,

Electronic signature: /Matthew H. Grady/

Matthew H. Grady

Registration No.: 52,957

John N. Anastasi

Registration No.: 37,765

LANDO & ANASTASI LLP

Riverfront Office Park

One Main Street

Suite 1100

Cambridge, Massachusetts 02142

(617) 395-7000

Attorneys for Applicant

PATENT COOPERATION TREATY

PCT

From the INTERNATIONAL SEARCHING AUTHORITY

NOTIFICATION OF TRANSMITTAL OF
THE INTERNATIONAL SEARCH REPORT AND
THE WRITTEN OPINION OF THE INTERNATIONAL
SEARCHING AUTHORITY, OR THE DECLARATION

To:
Donahoe, Robert V.
LANDO & ANASTASI, LLP
Riverfront Office Park
One Main Street, Eleventh Floor Suite 1100
Cambridge, MA 02142
ETATS-UNIS D'AMERIQUE

(PCT Rule 44.1)

Date of mailing (day/month/year)		20 January 2012 (20-01-2012)
Applicant's or agent's file reference W0537-7018WO	FOR FURTHER ACTION	See paragraphs 1 and 4 below
International application No. PCT/US2011/051966	International filing date (day/month/year)	16 September 2011 (16-09-2011)
Applicant UNIVERSAL SECURE REGISTRY, LLC		

1. The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

Filing of amendments and statement under Article 19:
The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

When? The time limit for filing such amendments is normally two months from the date of transmittal of the International Search Report.

Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes
1211 Geneva 20, Switzerland, Facsimile No.: (41-22) 338.82.70

For more detailed instructions, see PCT Applicant's Guide, International Phase, paragraphs 9.004 - 9.011.

2. The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. **With regard to any protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Reminders**

The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. Following the expiration of 30 months from the priority date, these comments will also be made available to the public.


Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the international Bureau before completion of the technical preparations for international publication (Rules 90bis.1 and 90bis.3).

Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

For details about the applicable time limits, Office by Office, see www.wipo.int/pct/en/texts/time_limits.html and the *PCT Applicant's Guide*, National Chapters.

RECEIVED
JAN 23 2011
L-4

Name and mailing address of the International Searching Authority  European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040 Fax: (+31-70) 340-3016	Authorized officer DE JONG, Coen Tel: +31 (0)70 340-2015
--	--

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference W0537-7018WO	FOR FURTHER ACTION see Form PCT/ISA/220 as well as, where applicable, item 5 below.	
International application No. PCT/US2011/051966	International filing date (day/month/year) 16/09/2011	(Earliest) Priority Date (day/month/year) 17/09/2010
Applicant UNIVERSAL SECURE REGISTRY, LLC		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 3 sheets.

It is also accompanied by a copy of each prior art document cited in this report.

1. Basis of the report

a. With regard to the **language**, the international search was carried out on the basis of:

- the international application in the language in which it was filed
 a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))

b. This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6bis(a)).

c. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. **Certain claims were found unsearchable** (See Box No. II)

3. **Unity of invention is lacking** (see Box No III)

4. With regard to the **title**,

- the text is approved as submitted by the applicant
 the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

- the text is approved as submitted by the applicant
 the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings**,

- a. the figure of the **drawings** to be published with the abstract is Figure No. 12
 as suggested by the applicant
 as selected by this Authority, because the applicant failed to suggest a figure
 as selected by this Authority, because this figure better characterizes the invention
- b. none of the figures is to be published with the abstract

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2011/051966

A. CLASSIFICATION OF SUBJECT MATTER INV. H04L29/06 H04W12/06 ADD.		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) H04W H04L		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used) EPO-Internal		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2010/000455 A1 (VODAFONE HOLDING GMBH [DE]; MOUTARAZAK SAID [NL]; KORAICHI NAJIB [NL]) 7 January 2010 (2010-01-07) page 3, lines 6-23; claim 4 page 4, lines 28-31 page 5, lines 27-30	1-33
A	US 2007/186115 A1 (GAO XIANG [CN] ET AL) 9 August 2007 (2007-08-09) paragraphs [0008], [0072], [0074]	1-33
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family annex.		
* Special categories of cited documents :		
"A" document defining the general state of the art which is not considered to be of particular relevance "E" earlier document but published on or after the international filing date "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) "O" document referring to an oral disclosure, use, exhibition or other means "P" document published prior to the international filing date but later than the priority date claimed		"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art. "&" document member of the same patent family
Date of the actual completion of the international search <p align="center">12 January 2012</p>		Date of mailing of the international search report <p align="center">20/01/2012</p>
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Fax: (+31-70) 340-3016		Authorized officer <p align="center">Veen, Gerardus</p>

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2011/051966

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2010000455 A1	07-01-2010	AT 531220 T	15-11-2011
		EP 2152033 A1	10-02-2010
		US 2011113476 A1	12-05-2011
		WO 2010000455 A1	07-01-2010

US 2007186115 A1	09-08-2007	NONE	

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

PCT

To:

see form PCT/ISA/220

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**
(PCT Rule 43*bis*.1)

Date of mailing
(*day/month/year*) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference see form PCT/ISA/220	FOR FURTHER ACTION See paragraph 2 below
---	--

International application No. PCT/US2011/051966	International filing date (<i>day/month/year</i>) 16.09.2011	Priority date (<i>day/month/year</i>) 17.09.2010
--	---	---

International Patent Classification (IPC) or both national classification and IPC
INV. H04L29/06 H04W12/06

Applicant
UNIVERSAL SECURE REGISTRY, LLC

1. This opinion contains indications relating to the following items:

- Box No. I Basis of the opinion
- Box No. II Priority
- Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- Box No. IV Lack of unity of invention
- Box No. V Reasoned statement under Rule 43*bis*.1(a)(i) with regard to novelty, inventive step and industrial applicability; citations and explanations supporting such statement
- Box No. VI Certain documents cited
- Box No. VII Certain defects in the international application
- Box No. VIII Certain observations on the international application



2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1*bis*(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

<p>Name and mailing address of the ISA:</p> <div style="text-align: center;">  </div> <p>European Patent Office P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk - Pays Bas Tel. +31 70 340 - 2040 Fax: +31 70 340 - 3016</p>	<p>Date of completion of this opinion</p> <p>see form PCT/ISA/210</p>	<p>Authorized Officer</p> <p>Veen, Gerardus</p> <p>Telephone No. +31 70 340-3811</p> <div style="text-align: right;">  </div>
--	---	--

Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:
 - the international application in the language in which it was filed
 - a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).
2. This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1 (a))
3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, this opinion has been established on the basis of a sequence listing filed or furnished:
 - a. (means)
 - on paper
 - in electronic form
 - b. (time)
 - in the international application as filed
 - together with the international application in electronic form
 - subsequently to this Authority for the purposes of search
4. In addition, in the case that more than one version or copy of a sequence listing has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
5. Additional comments:

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes: Claims	<u>1-33</u>
	No: Claims	
Inventive step (IS)	Yes: Claims	<u>1-33</u>
	No: Claims	
Industrial applicability (IA)	Yes: Claims	<u>1-33</u>
	No: Claims	
2. Citations and explanations
see separate sheet

**WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY**

International application No.
PCT/US2011/051966

Box No. VIII Certain observations on the international application

The following observations on the clarity of the claims, description, and drawings or on the question whether the claims are fully supported by the description, are made:

see separate sheet

Re Item V

Reasoned statement with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

The following documents are referred to in this communication:

- D1 WO 2010/000455 A1 (VODAFONE HOLDING GMBH [DE]; MOUTARAZAK SAID [NL]; KORAICHI NAJIB [NL]) 7 January 2010 (2010-01-07)
- D2 US 2007/186115 A1 (GAO XIANG [CN] ET AL) 9 August 2007 (2007-08-09)

1 D1, regarded as the closest prior art, discloses a method and system for controlling access to restricted resources by means of a time-dependent password which is generated in a handheld communication device, after validating an authentication code entered by a user. The most relevant passages are cited in the search report.

The subject-matter of present claim 1 differs from D1 in that the password has a limited validity in the sense that the user is permitted to continue accessing the resource so long as computer operated by the user periodically receives subsequent authentication information from the handheld device. D1, on the other hand, is silent as to how long a user is given access once a valid password has been entered.

The problem solved by the present invention may thus be defined as "how to increase the security of a one-time password access control system".

As none of the available prior art documents discloses or suggests a similar solution, the subject-matter of independent claim 1 of the present application is considered novel and inventive in the sense of Art. 33(2) and (3) PCT, respectively.

2 The same reasoning applies, mutatis mutandis, to independent claim 24 which is, therefore, also novel and inventive.

3 The remaining claims, 2-23 and 25-33, are all dependent and thus also novel and inventive.

4 As to D2, this document discloses a card to be entered into the card slot of a mobile phone, the card generating a time-dependent password, which is displayed on the phone display to be entered by the user into a computer keyboard.

Re Item VIII

Certain observations on the international application

5 Claim 21 is not clear (Art. 6 PCT) because it refers to itself.

Possible steps after receipt of the international search report (ISR) and written opinion of the International Searching Authority (WO-ISA)

General information

For all international applications filed on or after 01/01/2004 the competent ISA will establish an ISR. It is accompanied by the WO-ISA. Unlike the former written opinion of the IPEA (Rule 66.2 PCT), the WO-ISA is not meant to be responded to, but to be taken into consideration for further procedural steps. This document explains about the possibilities.

Amending claims under Art. 19 PCT

Within 2 months after the date of mailing of the ISR and the WO-ISA the applicant may file amended claims under Art. 19 PCT directly with the International Bureau of WIPO. The PCT reform of 2004 did not change this procedure. For further information please see Rule 46 PCT as well as form PCT/ISA/220 and the corresponding Notes to form PCT/ISA/220.

Filing a demand for international preliminary examination

In principle, the WO-ISA will be considered as the written opinion of the IPEA. This should, in many cases, make it unnecessary to file a demand for international preliminary examination. If the applicant nevertheless wishes to file a demand this must be done before expiry of 3 months after the date of mailing of the ISR/ WO-ISA or 22 months after priority date, whichever expires later (Rule 54bis PCT). Amendments under Art. 34 PCT can be filed with the IPEA as before, normally at the same time as filing the demand (Rule 66.1 (b) PCT).

If a demand for international preliminary examination is filed and no comments/amendments have been received the WO-ISA will be transformed by the IPEA into an IPRP (International Preliminary Report on Patentability) which would merely reflect the content of the WO-ISA. The demand can still be withdrawn (Art. 37 PCT).

Filing informal comments

After receipt of the ISR/WO-ISA the applicant may file informal comments on the WO-ISA directly with the International Bureau of WIPO. These will be communicated to the designated Offices together with the IPRP (International Preliminary Report on Patentability) at 30 months from the priority date. Please also refer to the next box.

End of the international phase

At the end of the international phase the International Bureau of WIPO will transform the WO-ISA or, if a demand was filed, the written opinion of the IPEA into the IPRP, which will then be transmitted together with possible informal comments to the designated Offices. The IPRP replaces the former IPER (international preliminary examination report).

Relevant PCT Rules and more information

Rule 43 PCT, Rule 43bis PCT, Rule 44 PCT, Rule 44bis PCT, PCT Newsletter 12/2003, OJ 11/2003, OJ 12/2003



(51) International Patent Classification:
H04W 12/06 (2009.01)

(74) Agent: JOSTARNDT PATENTANWALTS-AG; Brüssel-
seler Ring 51, D-52074 Aachen (DE).

(21) International Application Number:
PCT/EP2009/004744

(81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ,
CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO,
DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP,
KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD,
ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI,
NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD,
SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT,
TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(22) International Filing Date:
1 July 2009 (01.07.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
08011848.2 1 July 2008 (01.07.2008) EP

(71) Applicant (for all designated States except US): VODA-
PHONE HOLDING GMBH [DE/DE]; Mannesmannufer
2, 40213 Düsseldorf (DE).

(84) Designated States (unless otherwise indicated, for every
kind of regional protection available): ARIPO (BW, GH,
GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM,
ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ,
TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE,
ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV,
MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM,

(72) Inventors; and
(75) Inventors/Applicants (for US only): MOUTARAZAK,
Said [NL/NL]; Portonnekuilstraat 18, 6163 BP Geleen
(NL). KORAICHI, Najib [NL/NL]; Kruisstraat 38,
NL-6333 CT Schimmert (NL).

[Continued on next page]

(54) Title: METHOD AND DEVICE FOR GENERATING A TIME-DEPENDENT PASSWORD

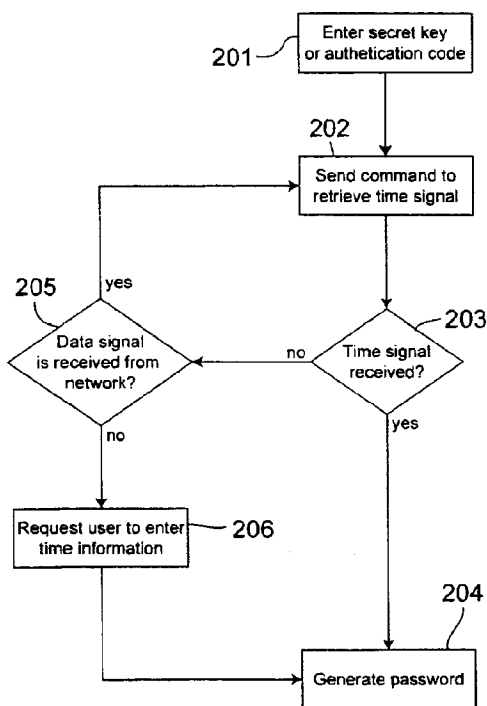


Fig. 2

(57) Abstract: The invention relates to the generation of a time-dependent password using an external time signal. For generating a time-dependent password in a temporary absence of the external time signal, the invention proposes a method comprising the steps of: - checking, whether the security device has access to an external time signal; - requesting a user of the security device to enter time information, if it is determined that the security device has no access to the external time signal; and - generating a time-dependent password using the time information entered in response to the request. The invention further relates to a device for performing the method.

WO 2010/000455 A1

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG). **Published:**

— with international search report (Art. 21(3))

Declarations under Rule 4.17:

— of inventorship (Rule 4.17(iv))

Method and device for generating a time-dependent password

5

Technical Field

The invention relates to the generation of time-dependent passwords, particularly to the generation of time-synchronized one-time passwords. More specifically, the invention relates to a method for generating a time-dependent password in a mobile communication device. The invention further relates to a device for generating a time-dependent password in a mobile communication device and to a mobile communication device comprising the device.

15

Background of the Invention

Conventional static passwords bear the risk to be discovered by unauthorized third parties. Protection against unauthorized access to restricted resources can be improved by using so-called one-time passwords (OTPs), which are valid only for one time. An OTP mechanism, commonly referred to as time-synchronised type OTP, involves synchronised time information for generating and validating OTPs. In regular time intervals, such as, for example, every minute, a security device or an application, which is usually called "token", generates a new OTP from current time information and a secret key assigned to the user. For validating the OTP, an authorisation station re-generates the OTP based on the secret key and own current time information using the same algorithm as the token and compares the self-generated password with the password generated by the token.

30 In the OTP environment described before, the time information used in the token and the time information used in the authorisation station have to be well synchronised. However, in OTP environments, certain time deviations are al-

lowed, which means that the authorisation station accepts OTPs generated and based on time information that differs from that time of the authorisation station by a predefined time deviation. Typical allowed time deviations may be in the range of one or several minutes, for example.

5

The token may be a closed, tamper-resistant hardware system dedicated to the generation of OTPs, which stores the secret key of the user and which usually has a built-in clock for providing the time information. As an alternative, the token may be configured as a so-called "soft token", which is a software application run on a general-purpose processor.

10

The international patent application WO 2007/126227 describes a mobile communication device, such as, for example, a mobile phone or a PDA (Personal Data Assistant) or the like, which has an interface for accepting an IC chip (IC: Integrated Circuit) for generating time-synchronised type OTPs. The IC chip stores the user's secret key and comprises a module for generating the OTPs. The time information is provided by a base station and received by the radio frequency processing unit of the mobile communication device.

15

The IC chip allows for implementing the token for generating time-synchronised type OTPs in a mobile communication device. An external time signal provides the time information for generating the OTPs, such that a special clock for this purpose can be dispensed with. However, the time information is available only if the mobile communication device is connected to the base station. This means that the generation of OTPs is not possible, if the mobile communication device cannot be connected to the base station.

20
25

Summary of the Invention

Therefore, it is an object of the present invention to allow for generating time-synchronised type OTPs in a device having access to an external time signal, when the device cannot receive the external time signal.

30

The object is achieved by a method comprising the features of claim 1 and by a device comprising the features of claim 12. Embodiments of the method and the device are given in the dependent claims.

5

According to a first aspect of the invention, a method of the type described before is proposed, which comprises the following steps:

- checking, whether the security device has access to an external time signal;
 - requesting a user of the security device to enter the time information, if it is determined that the security device has no access to the external time signal; and
 - generating a time-dependent password using the time information entered in response to the request.
- 10

15 According to a second aspect, the invention proposes a device for generating a time-dependent password using time information. The device comprises:

- a checking means for checking, whether an external time signal is accessible;
 - a requesting means for requesting a user to enter the time information, if the checking means determines that the external time signal is not accessible, and
 - a calculation means for generating a time-dependent password using the time information entered in response to the request.
- 20

25 The invention has the advantage that a time-dependent password can be generated in the absence of the external time signal. This is achieved by allowing the user of the security device to specify the time information needed for generating a time-dependent password, if no external time signal is received in the mobile communication device.

30

By allowing the user to input the time information, the invention contradicts the usual opinion that the mechanism for generating the time information needed

for calculating time-dependent passwords is a sensitive component of the password generation, which has to be secured against access by the user. Particularly, it has been discovered that the possibility to generate a time-dependent password based on the time information provided by the user is very
5 useful to bridge a temporarily absence of an external time signal.

However, if the external time signal can be received in the security device, the time signal can be used for generating the time-dependent password. This has the advantage that the risk of fraudulent misuse is reduced.
10

Therefore, in one embodiment of the method and the device, the time-dependent password is generated using the external time signal, if it is determined that the security device has access to the external time signal.

15 The time information used for generating the time-dependent password has to be synchronized with the time information used by the authorization station. However, the user may stay in a time zone different from the time zone in which the authorization station is located. If, in this case, the user entered his local time, the generated password would be invalid due to the time difference to the
20 location of the authorization station.

Therefore, in one embodiment of the method and the device, the user is requested to specify a time zone to which the entered time information refers, the time information entered by the user is converted to the time zone of an authorization station for validating the password and the time-dependent password is
25 generated using the converted time information.

In a further embodiment of the method and the device, the user is requested to enter an authentication code and the entered time information is only used for
30 generating a time-dependent password, if the authentication code has been validated successfully.

This prevents an unauthorized third party that does not dispose of the authentication code from generating a password and making fraudulent use of it. Particularly, an unauthorized third party is prevented from generating and using a password that is valid in a future point in time.

5

Furthermore, one embodiment of the method and the device comprises the steps of:

- storing the entered time information;
- determining that the security device has access to the external time signal;
- 10 - checking, whether the entered time information refers to a future point in time compared to the currently received external time signal; and
- initiating an alarm routine, if the entered time information refers to a future point in time compared to the currently received time signal.

- 15 This provides security against an attack based on the aforementioned generation of a password, which is valid in a future point in time.

In order to prevent an attacker from gaining unauthorized access using such a password, in one embodiment of the method and the device, the password
20 generated using the entered time information is being marked as invalid in the authorization station in response to the initiation of the alarm routine.

In a further embodiment of the method and the device, the user is requested to enter a secret key allocated to the user and the time-dependent password is
25 generated using the secret key entered by the user.

Moreover, in one embodiment of the method and the device, the generated time-dependent password is displayed at the security device and/or the time-dependent password is transmitted from the security device to the authorisation
30 station via a data network to which the security device is connected.

In one embodiment of the method, a mobile communication device comprises the security device.

5 Using a mobile communication device comprising security device for the generating the time-dependent password increases the user convenience, since a user who usually carries a mobile communication device does not need an additional device for generating the time-dependent password.

10 In one embodiment of the method and the device, the external time signal may be provided by the communication network to which the security device can be connected. Therefore, in this embodiment checking, whether the security device has access to the external time signal, comprises checking, whether the security device is connected to a communication network providing the external time signal.

15 Providing the external time signal in the communication network has the advantage that no additional equipment is needed to access the time signal, if a mobile communication device comprises the security device, since the mobile communication device usually has all components for connecting to a communication network.

20

In one embodiment of the invention, the device is a smartcard, which can be connected to a mobile communication device.

25 It is an advantage of this embodiment that the device can be provided to the user easily in the form of smartcard, which is connectable to his mobile communication device. The usage of a mobile communication device for generating the time-dependent password is especially convenient for the user due to the reasons described before. One further advantage of this embodiment is that the security mechanism of the smartcard prevents fraudulent use of the device.

30

In mobile communication, smartcards are used for identifying and authenticating a user to a mobile communication network. Advantageously, such smartcards can also host the device according to the invention. Therefore, in one embodiment of the invention, the smartcard comprises a subscriber identification module for identifying and/or authenticating a user to a mobile communication network.

Furthermore, the invention provides a computer program comprising software code portions for performing a method of the type described before, when the computer program is run on a processor.

Moreover, the invention proposes a mobile communication device comprising a device of the type before.

These and other aspects of the invention will be apparent from and elucidated with reference to the embodiments described hereinafter making reference to the accompanying drawings.

Brief Description of the Drawings

20

In the drawings

Fig. 1 is a schematic block diagram showing a mobile communication device for generating time-synchronised type OTPs, and

25

Fig. 2 is a schematic flow chart illustrating a method for providing time information for generating the time-synchronised type OTPs.

Detailed Description of Embodiments of the Invention

30

Figure 1 shows a mobile communication device 101, which can be connected to a mobile communication network (PLMN – Public Land Mobile Network) 102,

which may be configured according to the GSM or UMTS standard, for example (GSM: Global System for Mobile communications; UMTS: Universal Mobile Telecommunications System). For connecting the mobile communication device 101 to the PLMN 102, the mobile communication device 101 comprises a radio interface 103. The radio interface 103 is coupled to a main processor 104 for controlling the operation of the mobile communication device 101. For interacting with the mobile user, the mobile communication device 101 comprises an input component 105 and a display component 106 both coupled to the main processor 104. Applications run by the main processor 104 and reference data are stored in a memory component 107 to which the main processor 104 has access.

The mobile communication device 101 interacts with a smartcard 108, which is inserted into a card reader unit 114 of the mobile communication device 101. The smartcard 108 includes a microprocessor 109 and a memory 110 and comprises a subscriber identification module allocated to the user of the mobile communication device 101. Particularly, the subscriber identification module includes information for identifying and authenticating the mobile user to the PLMN 102 and provides functionality for accessing services of the PLMN 102. The subscriber identification module may be configured in accordance with the type of the PLMN 102. If the PLMN 102 is a GSM or UMTS network, the subscriber identification module is a subscriber identity module (SIM) according to the GSM standard or a universal subscriber identity module (USIM) according to the UMTS standard.

The mobile user has the authorisation to access a restricted resource. In one embodiment, the resource may be a web application or a web service hosted by a network server 113, which is connected to a data network 112. Access to the resource is controlled by an authorisation station 111, which denies access to the resource unless the user is identified and authenticated successfully. The network server 113 may comprise the authorisation station 111, or the authorisation station 111 may reside in another network server. In the embodiment

depicted in figure 2, the network server 112 is connected to the data network 112 via the authorisation station 111. However, other network architectures are possible.

- 5 The authorisation station 111 performs the user authorisation using time-synchronised OTPs. This ensures a relatively high level of security of the access control. Thus, the web application may be a payment application, for example, that has to be secured efficiently against unauthorised access by third parties.

10

For generating time-synchronised OTPs, the mobile communication device 101 comprises an OTP application. The OTP application may be resident in the mobile terminal and run on the main processor 104 of the mobile communication device 101. In a different embodiment, the OTP application is resident in the smartcard 108 including the subscriber identification module. In this embodiment, the OTP application is stored in the memory 110 and run on the micro-processor 109 of the smartcard 108. This has the advantage that the OTP application is secured against unauthorised access by means of the security mechanism of the smartcard 108. In further embodiments, an OTP chip including the OTP application may be removably connected to the mobile terminal.

15

20

The mobile communication device 101 may be connected to the data network 112 via an access technology, such as, for example, a WLAN connection. In figure 1, this is schematically illustrated by means of the arrow 115. In this architecture, the mobile user may access the network server 113 using the mobile communication device 101 and OTPs generated in the mobile communication device 101 may be transmitted electronically from the mobile communication device 101 to the authorisation station 111. Furthermore, the PLMN 102 may be coupled to the data network 112, such that the mobile communication device 101 can be connected to the data network via the PLMN 102, if it is registered in the PLMN 102.

25

30

In another embodiment, the mobile user accesses the network server 113 using a further device connected to the data network 112, such as, for example, a personal computer. In this case, the OTP application outputs generated passwords at the mobile communication device 101. The user reads that generated
5 password at the display component 106 of the mobile communication device 101 and enters the password at the device used for accessing the network server 113.

The OTP application provides a graphical user interface at the display component 106 of the mobile communication device 101 for depicting outputs to the
10 user and for presenting input requests to the user. Moreover, the OTP application is configured to receive user inputs from the input component 105 of the mobile communication device 101. If the OTP application resides in the smart-card 108, the OTP application may access the functionalities of the mobile
15 communication device 101 using SIM Toolkit commands, which, in general, are known to a person skilled in the art.

For generating time-synchronised OTPs, an algorithm is implemented in the OTP application, which is used to calculate OTPs based on time information
20 and a secret key allocated to the user. The secret key may be a personal identification number (PIN), for example. The secret key may be entered by the user, when the OTP application is started or when the user requested the generation of a password. Likewise, it is possible that the secret key is stored securely in the mobile communication device 101, particularly in the smartcard 108. In this
25 embodiment, the generation of a password may be possible only after an authorisation code entered by the user has been validated successfully by the OTP application. The authorisation code may be another PIN and differs from the secret key allocated to the user in that the secret key is used to calculate the passwords, while the authorisation code is used to unlock the password
30 generation. Securing the OTP application with an authorisation code for unlocking the password generation has the advantage that an attacker has to use the mobile communication device 101 for generating passwords of the user, since

the secret key is secured against access within the mobile communication device 101.

For validating the password generated by the OTP application, the authorisation station 111 re-computes the passwords using the user's secret key, which is also stored in the authorisation station 111, and its own time information. The time information used by the OTP application and the time information present in the authorisation station 111 have to be synchronised accurately enough. Usually, the authorisation station 111 allows for generating passwords computed using a time information with a predetermined deviation from the time information present and authorisation station 111. For this purpose, the authorisation station 111 determines that the password is valid, if it is calculated using a time from a predetermined time interval around the current time of the authorisation station 111. The time interval may be between 1 and 15 minutes, preferably between 2 and 4 minutes.

The OTP application retrieves the time information needed for generating the time-synchronised OTPs from the PLMN 102. For this purpose, the PLMN 102 includes a supplementary service providing a time signal. The service may be accessed using so-called USSD commands (USSD: Unstructured Supplementary Service Data), which are, in general, known to a person skilled in the art in general. However, retrieving the time information from the PLMN 102 requires that the mobile communication device 101 was connected to the PLMN 102. This is not always true, since it may happen that the mobile communication device 101 is out of coverage of the PLMN 102, for example. Therefore, the OTP application requests the user to enter time information into the mobile communication device 101, in case no time information can be received from the PLMN 102.

In one embodiment, a method schematically depicted in figure 2 is implemented in the OTP application for this purpose: After the user has entered his secret key or his authorisation code in step 201, the OTP application sends a com-

mand to retrieve time information from the PLMN 102 in step 202. The command is passed to the radio interface 103 of the mobile communication device 101, which transmits the command to the PLMN 102, if the mobile communication device 101 is connected to the PLMN 102. After having passed the command to the radio interface 103 the OTP application checks, whether the command is responded within a predetermined time interval in step 203. This means that the OTP application checks, whether the time signal is received during the time interval. If the time signal is received in time, the OTP application computes a password based on the received time information and the secret key of the user in step 204.

If the OTP application determines in step 203 that no time information has been received from the PLMN 102 in the predetermined time interval, the OTP application checks, whether the mobile communication device 101 is connected to the PLMN 102 in step 205. This may be done by checking, whether the mobile communication device receives a predetermined data signal broadcasted in the PLMN 102, such as, for example, a signal identifying the PLMN 102. If it is determined in step 205 that the mobile communication device 101 is registered in the PLMN 102, the OTP application preferably goes back to step 202 and re-sends the command to retrieve the time information. However, if it is determined in step 205 that the mobile communication device 101 is not connected to the PLMN 102, the OTP application requests the user to enter time information at the mobile communication device 101. After having received the user input, the OTP application calculates a password using the time information specified by the user in step 204.

For requesting the user to input the time information, the user interface of the OTP application presented at the display component 106 of the mobile communication device may provide an input field, which may be filled in by the user using the input component 105 of the mobile communication device 101. The user may receive the time information from any available source. For example, this may be his wristwatch or a public watch in the vicinity of his position.

In order for the calculated password to be valid, the password has to be calculated using the time information present in the authorisation station 111. Particularly, this means that the time information used for the calculation should refer to the same time zone as the time information of the authorisation station 111. Therefore, in one embodiment, the user is requested to input a time information referring to the time zone of authorisation station 111 in step 206. This requires knowledge about the time zone of the authorisation station 111 and about the time shift between this time zone and the current time zone of the user.

10

In another embodiment, the user is requested to input his local time and to specify his current time zone. For the specification of the time zone, a list of the existing time zones may be presented to the user, such that the user can specify his time zone by choosing it from the list. Using the time information entered by the user and the information about the time zone the time information refers to, the OTP application calculates the local time of the authorisation station 111 and uses this calculated time to generate the password in step 204.

In order to prevent that an attacker uses the mobile communication device 101 to generate a password that will be valid in the future by inputting time information relating to a future point in time, the input of the time information by the user may be secured by an authorisation code. This means that the OTP application requests the user to enter the authorisation code besides the time information. The authorisation code is also stored securely in the mobile communication device 101, particularly in the smartcard 108. In this embodiment, the OTP application validates the authorisation code before generating a password using the time information given by the user.

Furthermore, in one embodiment, the OTP application stores at least the time information, when it calculates and outputs a password based on time information specified by the user. Particularly, the time information may be stored securely in the smartcard 108. After having stored the time information, the OTP

application monitors, whether the mobile communication device 101 connects to the PLMN 102 again. This may be done by sending commands to retrieve time information from the PLMN 102 or by checking in regular time intervals, whether a predetermined data signal broadcasted in the PLMN 102 is received in the
5 mobile communication device 101. Again, this data signal may be a signal identifying the PLMN 102 that is broadcasted in the PLMN in regular time intervals.

If the OTP application determines that the mobile communication device 101 is connected to the PLMN 102 again, the OTP application checks, whether the
10 time information used for calculating the password refers to a future point in time. If this is true, an alarm routine is started, since in this case an attacker might have generated the password for fraudulent use in the future. For the aforementioned check, the OTP application compares time information currently retrieved from the PLMN 102 and the stored time information. If it is determined
15 that the stored time information referred to the future compared to the currently received time information, the OTP application starts the alarm routine.

The alarm routine may comprise informing the user that a password has been generated for a future point in time. If the user judges that the password might
20 have been generated for fraudulent use, he may inform the authorization station 111. In another embodiment, the OTP application may inform the authorization station 111 automatically. For this purpose, the OTP application may generate a corresponding message specifying the time information in question, and the OTP application may control the mobile communication device 101 to transmit
25 the message to the authorisation station 111. The message may be transmitted to the authorisation station 111 via the PLMN 102 or via another data connection between the mobile communication device 101 and the authorisation station 111.

30 After having been informed about the possible misuse, steps can be taken in the authorisation station 111 to prevent an unauthorised access to the network server 113 using the password in question. This may be done by blocking ac-

cess to the network server 113 with this password. Particularly, the password generated for the future point in time may be marked as invalid, such that this password cannot be used as an authorisation for accessing the network server 113.

5

While the invention has been illustrated and described in detail in the drawings and foregoing description, such illustration and description are to be considered illustrative or exemplary and not restrictive; the invention is not limited to the disclosed embodiments. Particularly, the invention is not limited to a download
10 of an application or program code to smartcard 106. A person skilled in the art recognises that other data can be downloaded to the smartcard 106 in the same way as it has been described before in connection with the download of a program code of an application. Other variations to the disclosed embodiments can be understood and effected by those skilled in the art in practicing the claimed
15 invention, from a study of the drawings, the disclosure, and the appended claims.

In the claims, the word "comprising" does not exclude other elements or steps, and the indefinite article "a" or "an" does not exclude a plurality. A single processor or other unit may fulfill the functions of several items recited in the claims.
20 A computer program may be stored/distributed on a suitable medium, such as an optical storage medium or a solid-state medium supplied together with or as part of other hardware, but may also be distributed in other forms, such as via the Internet or other wired or wireless telecommunication systems. Any reference
25 signs in the claims should not be construed as limiting the scope.

Claims

1. A method for generating a time-dependent password in a security device (101; 108) using time information, the method comprising the steps of:
 - checking, whether the security device has access to an external time signal;
 - requesting a user of the security device to enter the time information, if it is determined that the security device has no access to the external time signal; and
 - generating a time-dependent password using the time information entered in response to the request.
2. The method according to claim 1, wherein the time-dependent password is generated using the external time signal, if it is determined that the security device (101; 108) has access to the external time signal.
3. The method according to one of the preceding claims, wherein the user is requested to specify a time zone to which the entered time information refers, wherein the time information entered by the user is converted to the time zone of an authorization station (111) for validating the password and wherein the time-dependent password is generated using the converted time information.
4. The method according to one of the preceding claims, wherein the user is requested to enter an authentication code and wherein the entered time information is only used for generating a time-dependent password, if the authentication code has been validated successfully.
5. The method according to one of the preceding claims, further comprising the steps of:
 - storing the entered time information;
 - determining that the security device (101; 108) has access to the external time signal;

- checking, whether the entered time information refers to a future point in time compared to the currently received external time signal; and
 - initiating an alarm routine, if the entered time information refers to a future point in time compared to the currently received time signal.
6. The method according to claim 5, wherein the password generated using the entered time information is marked as invalid in the authorization station (111) in response to the initiation of the alarm routine.
 7. The method according to one of the preceding claims, wherein the user is requested to enter a secret key allocated to the user and wherein the time-dependent password is generated using the secret key entered by the user.
 8. The method according to one of the preceding claims, wherein the generated time-dependent password is displayed at the security device (101; 108) and/or wherein the time-dependent password is transmitted from the security device (101; 108) to the authorisation station (111) via a data network to which the security device (101; 108) is connected.
 9. The method according to one of the preceding claims, wherein a mobile communication device (101) comprises the security device (101; 108).
 10. The method according to one of the preceding claims, wherein checking whether the security device (101; 108) has access to the external time signal comprises checking whether the security device (101; 108) is connected to a communication network (102) providing the external time signal.
 11. A computer program comprising software code portions for performing a method according to one of the preceding claims, when the computer program is run on a processor (104; 109).

12. A device (101; 108) for generating a time dependent password using time information comprising:
- a checking means for checking, whether an external time signal is accessible;
 - a requesting means for requesting a user to enter the time information, if the checking means determines that the external time signal is not accessible, and
 - a calculation means for generating a time-dependent password using the time information entered in response to the request.
13. A device (101; 108) according claim 12, wherein the device is a smartcard (108), which can be connected to a mobile communication device (101).
14. A device according to claim 13, wherein the smartcard (108) comprises a subscriber identification module for identifying and/or authenticating a user to a mobile communication network (102).
15. A mobile communication (101) device comprising a device (101; 108) according to one of the claims 12 to 14.

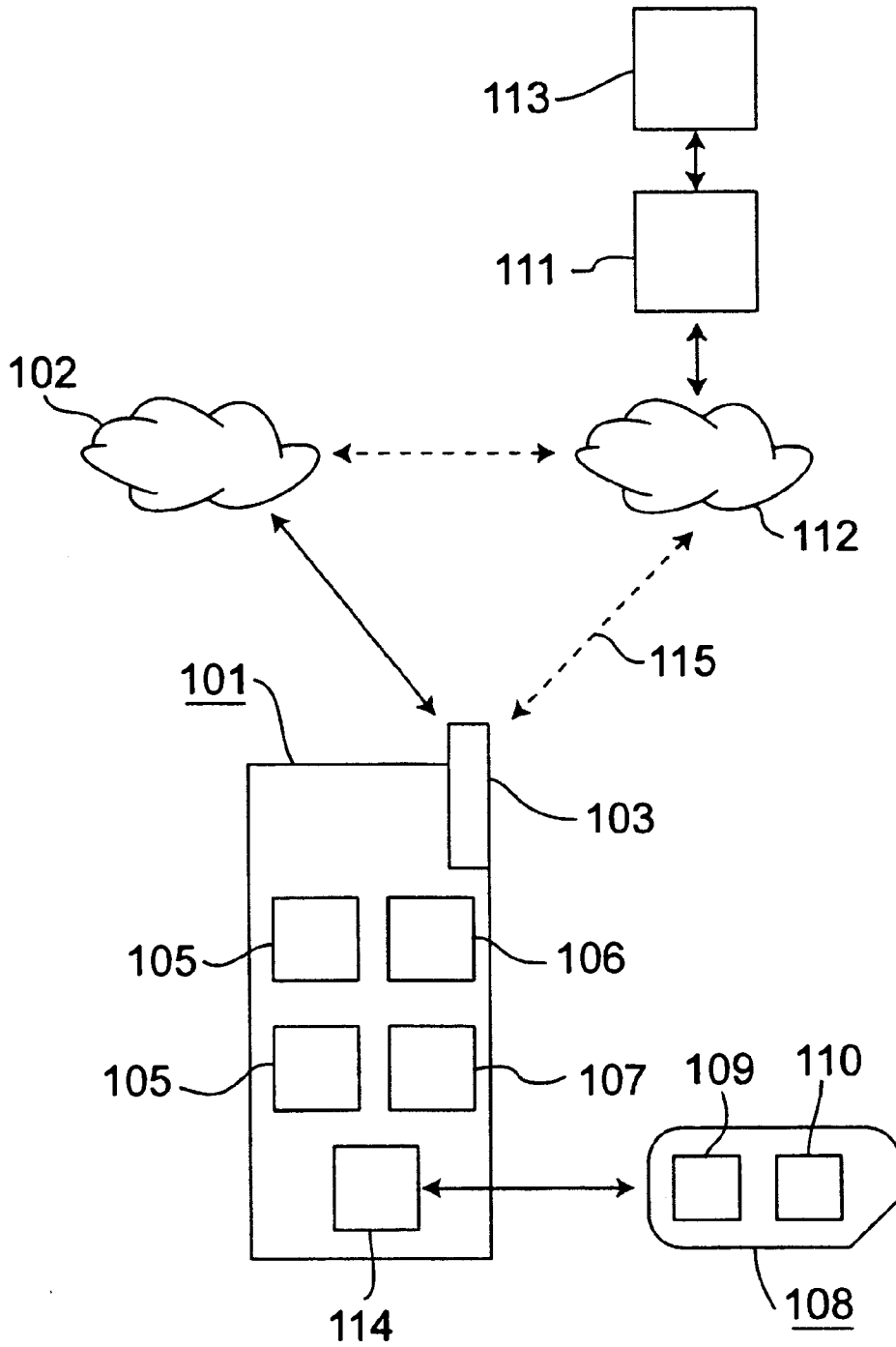


Fig. 1

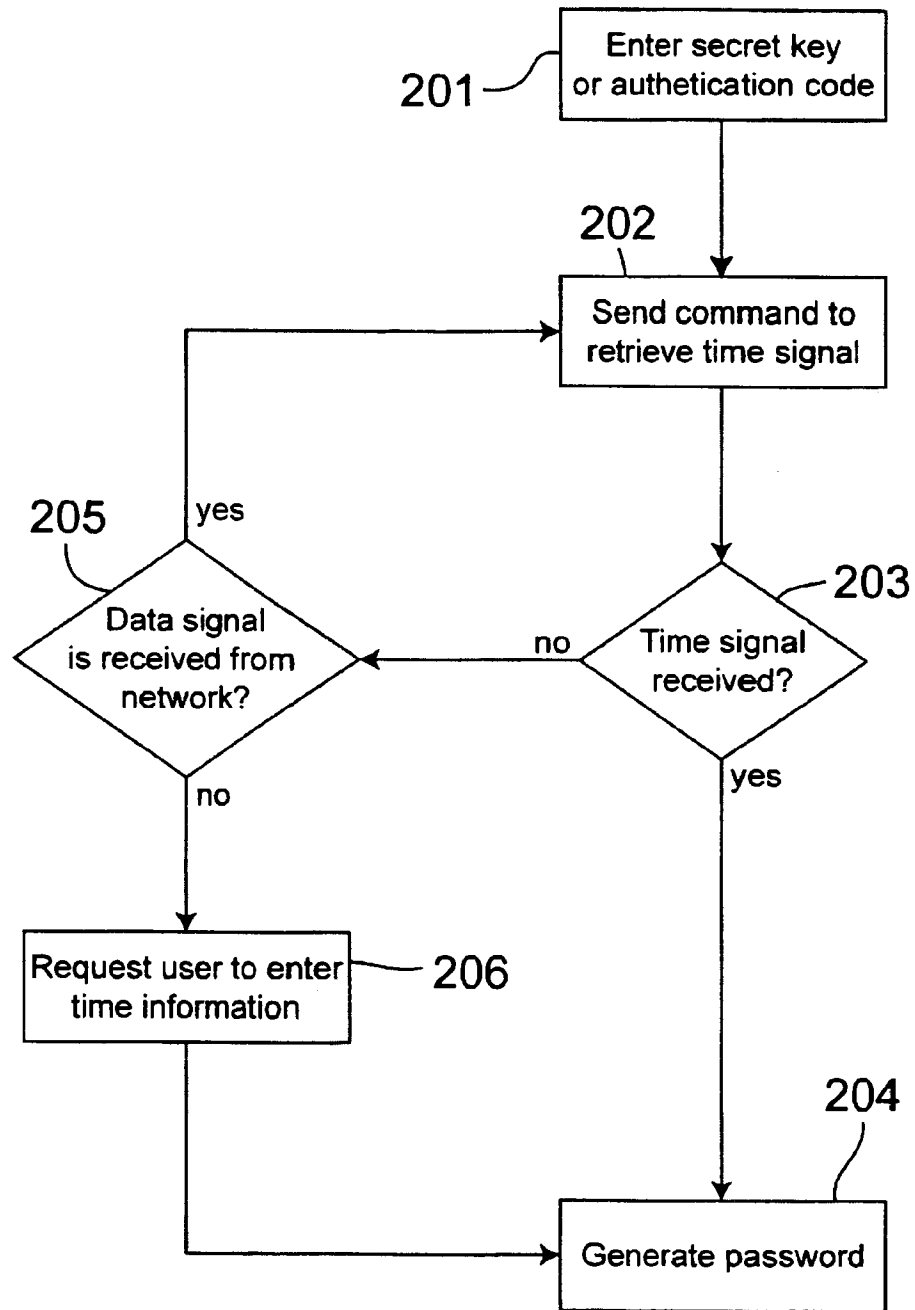


Fig. 2

INTERNATIONAL SEARCH REPORT

International application No
PCT/EP2009/004744

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04W12/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W G06F H04L G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2007/062787 A (VODAFONE HOLDING GMBH [DE]; JUNGBLUT STEPHAN [DE]) 7 June 2007 (2007-06-07) abstract page 5, line 18 - page 6, line 27 page 14, line 27 - page 19, line 11; figures 2,3	1-15
A	EP 1 833 219 A (MONITISE LTD [GB]) 12 September 2007 (2007-09-12) paragraphs [0014] - [0018] paragraphs [0030] - [0035] paragraphs [0043], [0044]	1-15
A	US 5 226 080 A (COLE JAMES F [US] ET AL) 6 July 1993 (1993-07-06) column 2, lines 27-50 column 5, line 3 - column 6, line 36	1-15

Further documents are listed in the continuation of Box C.

See patent family annex.

* Special categories of cited documents:

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *Z* document member of the same patent family

Date of the actual completion of the international search

25 September 2009

Date of mailing of the international search report

02/10/2009

Name and mailing address of the ISA/
European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Ruiz Sanchez, J

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2009/004744

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
WO 2007062787	A	07-06-2007	EP 1955515 A1	13-08-2008
EP 1833219	A	12-09-2007	WO 2007102005 A2	13-09-2007
US 5226080	A	06-07-1993	NONE	



US 20070186115A1

(19) **United States**

(12) **Patent Application Publication**
GAO et al.

(10) **Pub. No.: US 2007/0186115 A1**

(43) **Pub. Date: Aug. 9, 2007**

(54) **DYNAMIC PASSWORD AUTHENTICATION SYSTEM AND METHOD THEREOF**

Publication Classification

(75) Inventors: **Xiang GAO**, Beijing (CN); **Peng Hu**, Beijing (CN)

(51) **Int. Cl.**
H04K 1/00 (2006.01)

(52) **U.S. Cl.** 713/184

Correspondence Address:
SILICON VALLEY PATENT AGENCY
7394 WILDFLOWER WAY
CUPERTINO, CA 95014 (US)

(57) **ABSTRACT**

A dynamic password authentication system and the method thereof are disclosed. According to one aspect of the present invention, a dynamic password telecommunication card embedded with a security algorithm in the SIM card of a mobile telephone is used to generate a momentarily changed password. The technique as disclosed improves the security of identity authentication effectively and avoids the trouble for the user to remember the password and change the password frequently. The technique is also suitable to a systems that requires a higher security of the identify authentication, such as the bank, the securities, the police and the electronic government affair and the like, thereby to improve the security for the system administrator and the user to login the system.

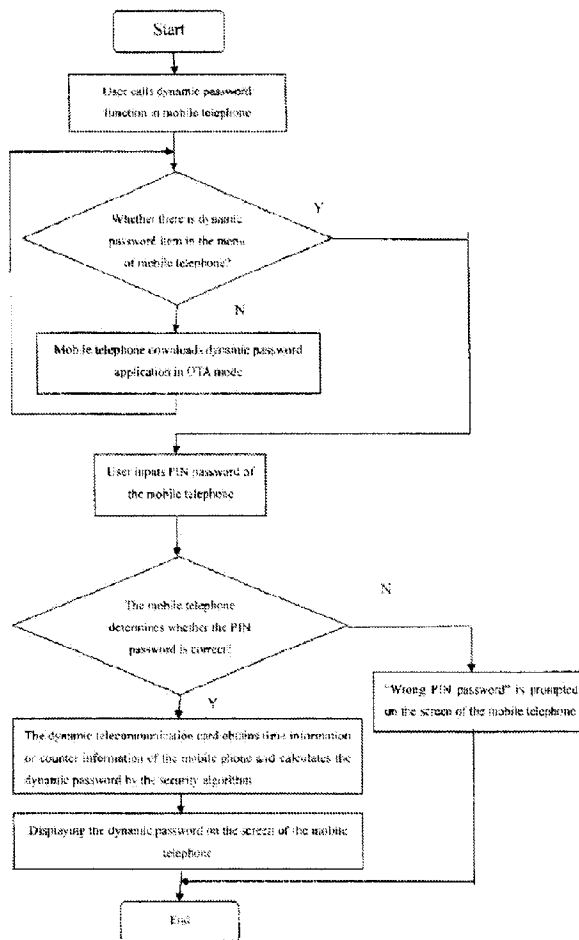
(73) Assignee: **Beijing Watch Data System Co., LTD.**, Beijing (CN)

(21) Appl. No.: **11/736,003**

(22) Filed: **Apr. 17, 2007**

(30) **Foreign Application Priority Data**

Oct. 20, 2005 (CN) PCT/CN05/01720



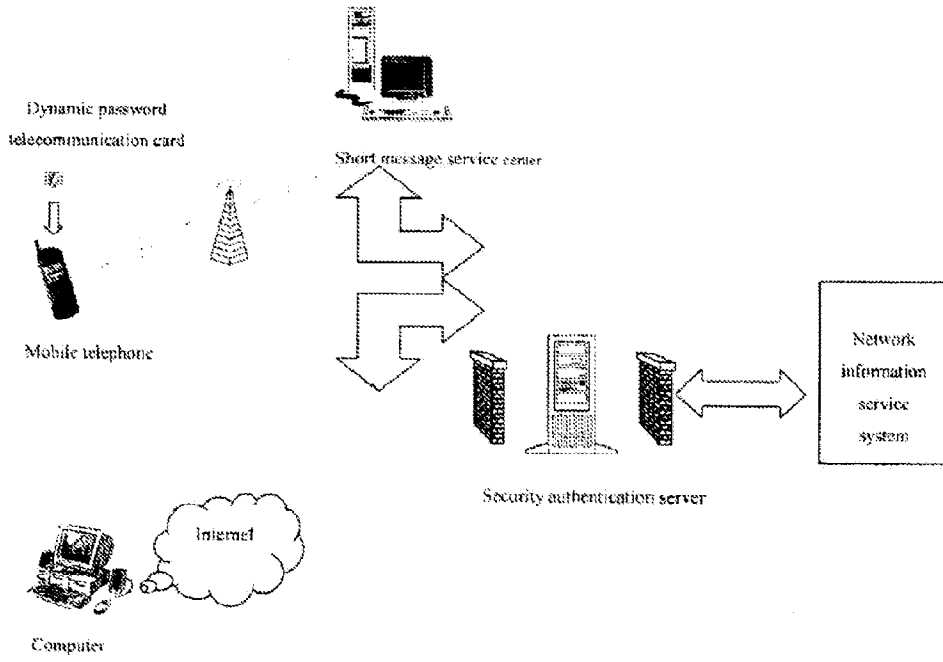


Fig. 1

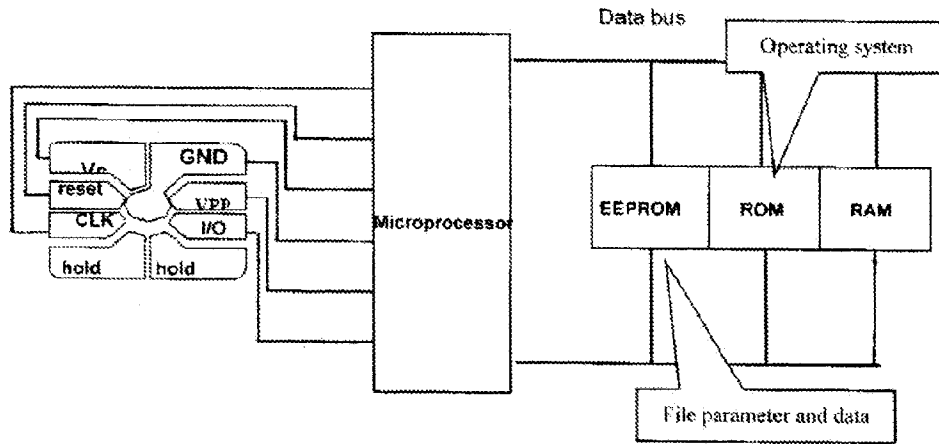


Fig.2

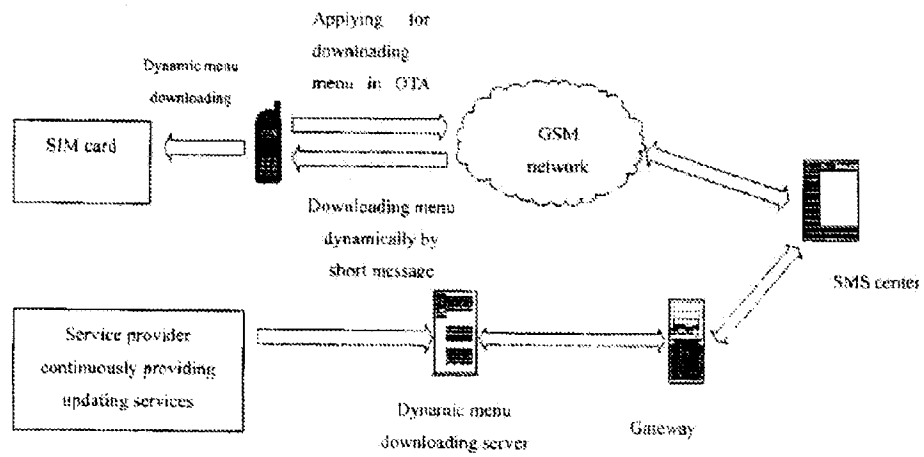


Fig.3

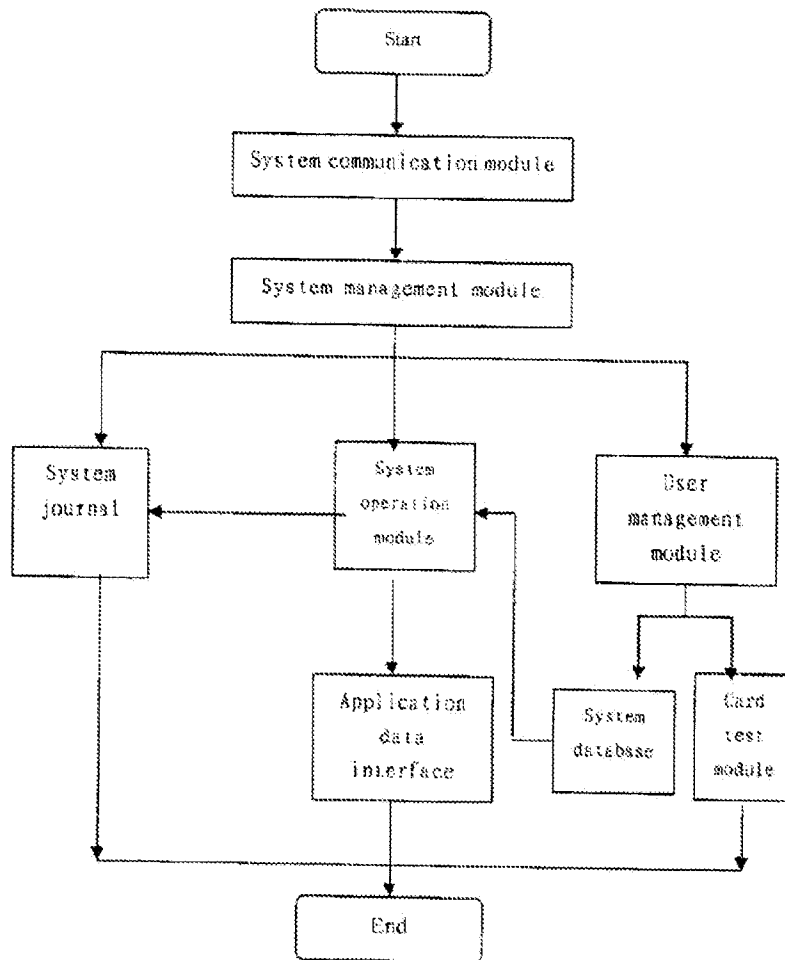


Fig.4

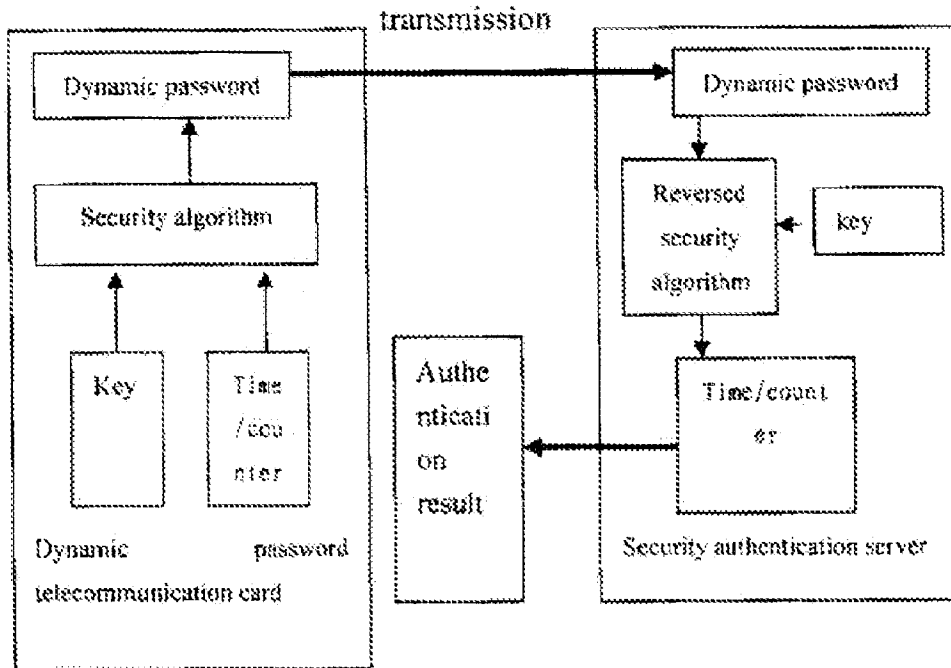


Fig.5

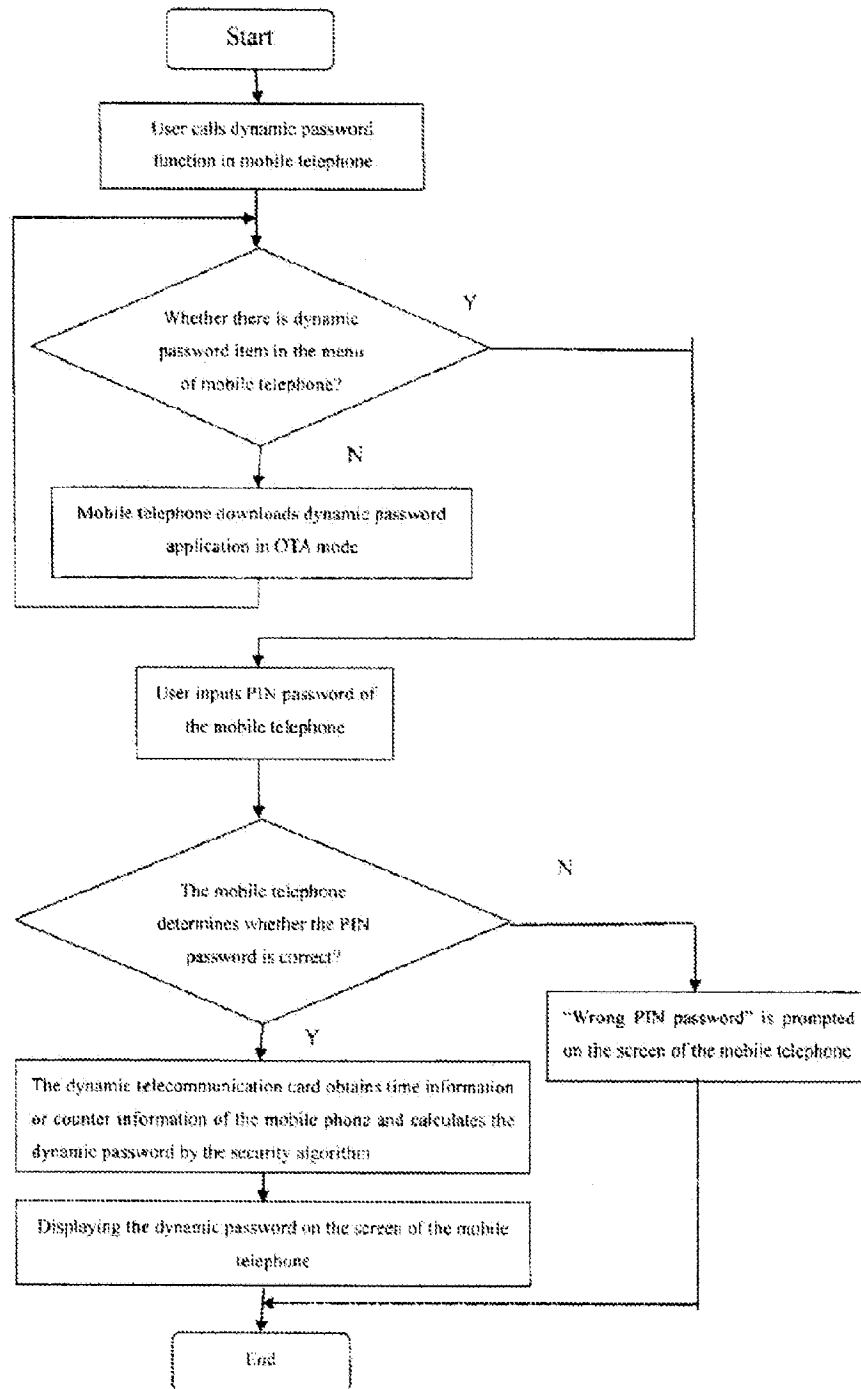


Fig.6

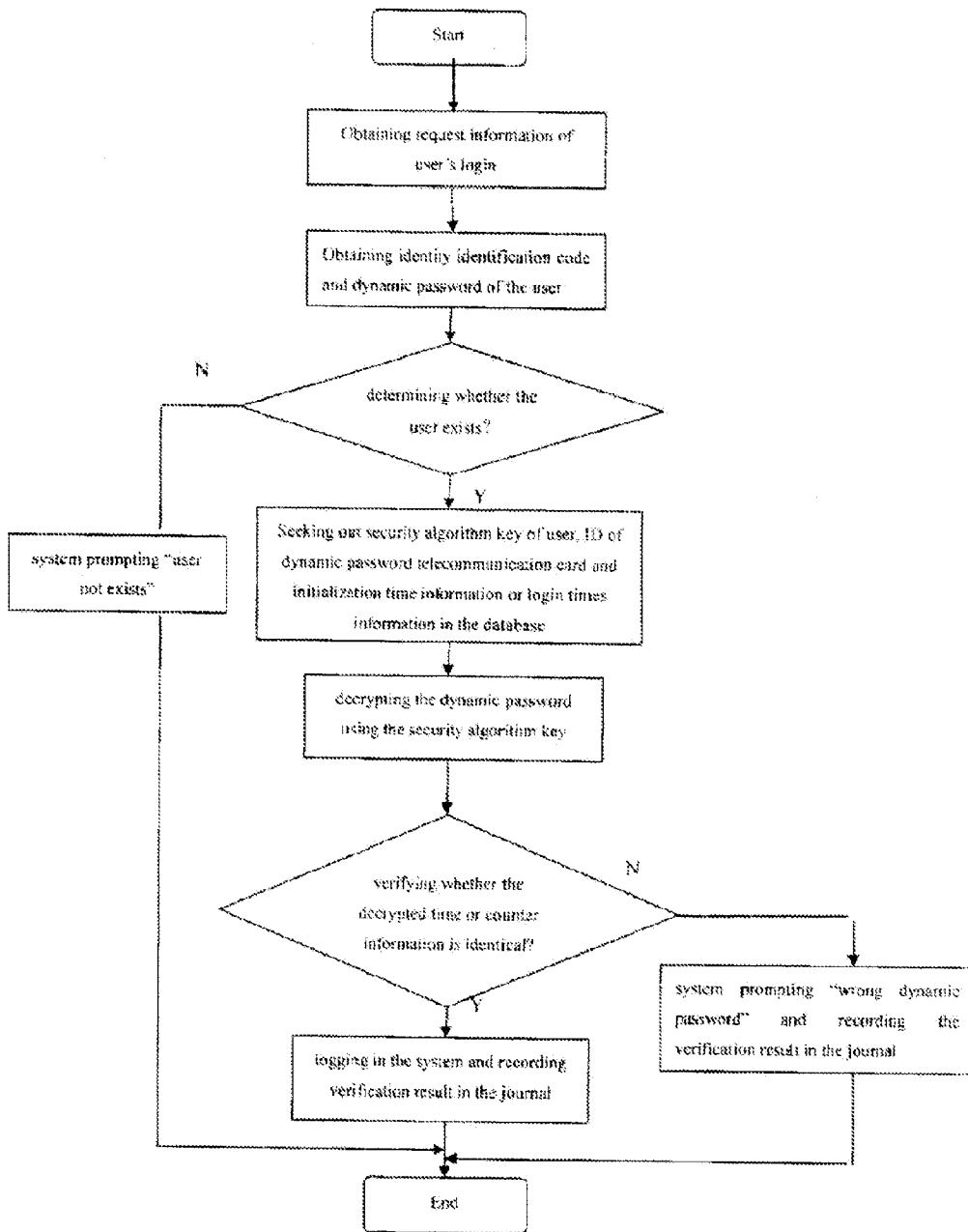


Fig.7

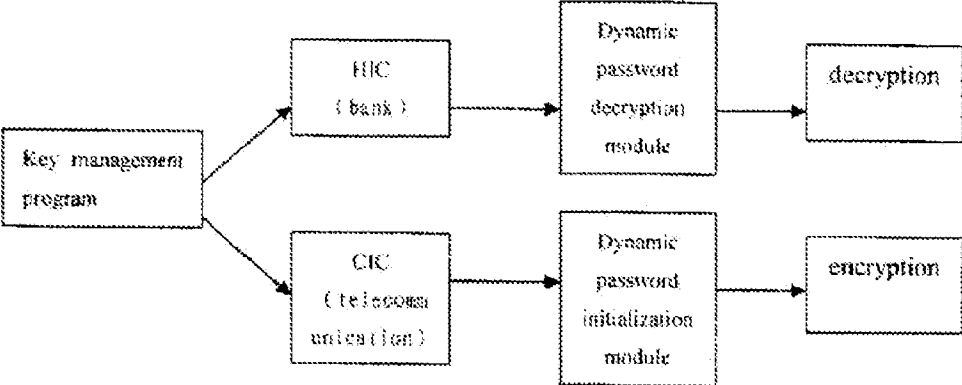


Fig.8

DYNAMIC PASSWORD AUTHENTICATION SYSTEM AND METHOD THEREOF

FIELD OF THE INVENTION

[0001] The present invention relates to the field of information security. In particular, the present invention relates to a dynamic password authentication system and the method thereof.

DESCRIPTION OF THE RELATED ART

[0002] With the rapid development of the computer and Internet technologies, many domestic large enterprises and government offices are trying to use the Internet to establish a fast and efficient network channel between the public and themselves in order to provide various network services to people. Due to the characteristics of the information service system based on the Internet, network security becomes more and more important. For example, in network bank, network tax reporting and network enterprise annual inspecting. In these systems, there is a large amount of information required to be kept secret. Thus, persons who access to these systems should be subject to strict identity authentication.

[0003] It is commonly understood that the identity authentication technology should be adopted in network information service systems. In addition, various technologies (for example, IC card technology and biology identify technology, fingerprint authentication) were applied in some systems to improve the reliability of the identity authentication. However, because of the restriction of some realistic conditions such as costs and technology maturity, currently a majority of systems still use the simple method based on user name+static password to perform the identity authentication.

[0004] Because the authentication mode based on the static password has the shortcomings of "unchangeable" and "easy to be decrypted", the method using the static password as a unique valid identity identification of a user in the network information service system can not meet the requirement on security. In addition, counterfeit user login is becoming increasingly problematic. Exemplary attacks to an authentication system based on the static password include network data stream sniffer, authentication information record/replay, dictionary attack, brute force, prying, social engineering and dumpster diving.

[0005] In recently years, a dynamic password technology has been proposed to remove the vulnerabilities in the static password. A continuously changing password is used to verify the identity of a user. The dynamic password token is kept with the user, and it is difficult for others to obtain dynamic password information in the token. In addition, the dynamic password is unpredictable, safe and convenient in use, and has a determined power and responsibility. Therefore, the technology can resolve the problem of identity authentication and authorization for remote and single time access required in network information service system.

[0006] However, the password token and backstage management system in this kind of dynamic password system is expensive and the system has a fixed renewal period. Further, dynamic password token used by the user has a single function, and the distribution, maintenance, replacement and

recovery of the token incurs an increase in expense and management cost to the user of the dynamic password system. For the above reasons, it is difficult for this kind of dynamic password system to be widely used in large numbers of general users.

SUMMARY OF THE INVENTION

[0007] This section is for the purpose of summarizing some aspects of the present invention and to briefly introduce some preferred embodiments. Simplifications or omissions in this section as well as the title and the abstract of this disclosure may be made to avoid obscuring the purpose of the section, the title and the abstract. Such simplifications or omissions are not intended to limit the scope of the present invention.

[0008] One aspect of the present invention is to provide a dynamic password authentication system and method thereof for using a mobile telephone, in which the user uses a dynamic password telecommunication card embedded with a security algorithm in the mobile telephone to generate a momentarily changed, unpredictable and one-off password.

[0009] Another aspect of the present invention is to provide a mechanism for transmitting a dynamic password function of a mobile telephone and a security authentication server by means of a mobile communication network. Thus, a shared secret between the mobile telephone and the security authentication server can be built in an OTA (Over-the-Air) mode, which can not be achieved by the conventional dynamic password token scheme.

[0010] A still another aspect of the present invention is to provide a dynamic password authentication system which can provide a dynamic password authentication in security.

[0011] Other objects, features, and advantages of the present invention will become apparent upon examining the following detailed description of an embodiment thereof, taken in conjunction with the attached drawings.

[0012] According to one embodiment, the present invention is a dynamic password authentication method, the method comprises: performing in a mobile terminal an encrypting operation using a dynamic password algorithm generating key and an initialization parameter stored in a telecommunication card to obtain an encryption result; sending the encryption result and a user identity identification code to a security authentication server; the security authentication server seeking out the dynamic password generating algorithm key in a database based on the user identity identification code and performing a decrypting operation to the encryption result to obtain a decrypted parameter, comparing the initialization parameter with the decrypted parameter, the mobile terminal passing the authentication if the initialization parameter is consistent with the decrypted parameter, and the authentication being denied if not.

[0013] The initialization parameter is time information of the mobile terminal. If the time information is used as the initialization parameter, a communication delay and a clock error value are added into the decrypted parameter.

[0014] The initialization parameter is counting information of the mobile terminal. In one embodiment, if the

counting information is used as the initialization parameter, an error value caused by the previous denying of the authentication is added.

[0015] The dynamic password generating algorithm key, a user menu or applications which are stored in the mobile terminal and the security authentication server are updated or changed in an Over-the-Air (OTA) mode.

[0016] The OTA mode comprises a service provider updating new services used with a dynamic password in a database of a download server, the mobile terminal implementing a momentary query to a dynamic menu download server by a mobile telephone short message, and sending a dynamic menu downloading request to the download server if new services used with the dynamic password are found, the request of the user being upload by network to the short message service center and transmitted to the download server by a gateway, the download server packaging the dynamic menu requested by the user into a short message with a specified format, and downloading the dynamic password menu required by the user into the dynamic password telecommunication card of the user through a network link in a data short message mode.

[0017] The telecommunication card may be a SIM card or a UIM card. A dynamic password authentication system comprises an authentication server, and a mobile terminal connected to the authentication server via wireless communication, the mobile terminal is provided with a dynamic password telecommunication card to generate a dynamic password, the authentication server is stored therein with a dynamic password key corresponding to the dynamic password telecommunication card of the mobile terminal to verify the dynamic password submitted by the mobile terminal.

[0018] The system further comprises a short message service center wirelessly connected to the mobile terminal, and the short message service center provides update service for the user of the mobile terminal or the authentication server.

[0019] A dynamic password is submitted to perform the identity authentication when a user of the present invention login the network information service system. Thus, problems concerning the user identity authentication in the remote/network environment are effectively resolved. In addition, the present invention can provide a convenient, wieldy, reliable and cost effective information security product for users.

[0020] The password download mode according to the present invention can realize a safety and frequent changing of the shared secret information between the mobile telephone and the security authentication server. It also can perform the updating and amending of the user menu and applications in the dynamic password telecommunication card to provide a convenient, rapid and low-cost download service for shared secret information of the users.

BRIEF DESCRIPTION OF THE DRAWINGS

[0021] The invention will be readily understood by the following detailed description in conjunction with the accompanying drawings, wherein like reference numerals designate like structural elements, and in which:

[0022] FIG. 1 is a schematic view showing a dynamic password authentication system based on a mobile telephone according to the present invention;

[0023] FIG. 2 is a schematic view showing a specific structure of a dynamic password telecommunication card used with the present invention;

[0024] FIG. 3 is a flow chart of the short message service center providing services in an OTA mode according to the present invention;

[0025] FIG. 4 is a schematic view showing a structure of a security server according to the present invention;

[0026] FIG. 5 is a schematic diagram showing a dynamic password authentication system based on a mobile telephone according to the present invention;

[0027] FIG. 6 is a flowchart of the mobile telephone generating a dynamic password according to the present invention;

[0028] FIG. 7 is a flowchart of the dynamic password authentication system authenticating a dynamic password according to the present invention; and

[0029] FIG. 8 is a flowchart of a password distribution of the dynamic password telecommunication card according to the present invention.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

[0030] The detailed description of the invention is presented largely in terms of procedures, steps, logic blocks, processing, and other symbolic representations that directly or indirectly resemble the operations of data processing devices coupled to networks. These process descriptions and representations are typically used by those skilled in the art to most effectively convey the substance of their work to others skilled in the art. Numerous specific details are set forth in order to provide a thorough understanding of the present invention. However, it will become obvious to those skilled in the art that the present invention may be practiced without these specific details. In other instances, well known methods, procedures, components, and circuitry have not been described in detail to avoid unnecessarily obscuring aspects of the present invention.

[0031] Reference herein to "one embodiment" or "an embodiment" means that a particular feature, structure, or characteristic described in connection with the embodiment can be included in at least one embodiment of the invention. The appearances of the phrase "in one embodiment" in various places in the specification are not necessarily all referring to the same embodiment, nor are separate or alternative embodiments mutually exclusive of other embodiments. Further, the order of blocks or steps in process flowcharts or diagrams representing one or more embodiments of the invention do not inherently indicate any particular order nor imply any limitations in the invention.

[0032] I. Description of the Structure of the Dynamic Password Authentication System Based on the Mobile Telephone

[0033] FIG. 1 is a schematic view showing a dynamic password authentication system based on a mobile telephone according to the present invention. As shown in FIG. 1, the

dynamic password authentication system mainly comprises a mobile phone, a dynamic password telecommunication card, a short message service center and a security authentication server.

[0034] 1. The Mobile Phone

[0035] At present, most of the mobile phones sold in the market can support the STK Class 2. A user with a mobile phone supporting the STK Class 2 can have services of the dynamic password authentication system based on the mobile telephone without special settings.

[0036] 2. Dynamic Password Telecommunication Card

[0037] Depending on implementation, the mobile phone uses a type of memory card (e.g., SIM card and UIM card) which is loaded with a module implementing a dynamic password security algorithm and can support a STK function (hereinafter referred as a "dynamic password telecommunication card"). The following description is taking the SIM card as an example. SIM (Subscriber Identity Model) card is also called a smart card or a user identity identification card, which is necessary for a GSM digital mobile phone to be used. The dynamic password telecommunication card according to the present invention is loaded with a module implementing a dynamic password security algorithm based on functions provided by the SIM card, and at the same time is stored therein with a user dynamic password key. In one instance, a calculating function of a microprocessor chip in the SIM card is configured to generate a one-off "dynamic password" with the time as a parameter, that is, according to the local time. In the other instance, a counter is used as a parameter to continuously and sequentially generate a one-off "dynamic password" which can not be predicted and tracked. Thus, the user password can not be stolen. In addition, the problem of frequently changing in the conventional password can also be resolved.

[0038] FIG. 2 is a schematic view showing an exemplary structure of a dynamic password telecommunication card used in some embodiments of the present invention. The dynamic password telecommunication card according to one embodiment comprises a microcircuit chip, in which not only is information concerning the user of the digital mobile phone stored, but also a dynamic password security algorithm and dynamic password key are loaded into its operating system. The microcircuit chip can perform an authenticating of a conventional GSM network to a subscriber identity and guarantee a normal communication of the subscriber strictly in conformity with the GSM international standard and criteria. At the same time, when the user calls a dynamic password function through the menu in the mobile telephone, if the PIN password verification is passed, the dynamic password telecommunication card uses the dynamic password key in the card to call a dynamic password security algorithm loaded in the operating system to calculate a dynamic password taking the time information in the mobile phone or accumulated counter information in the card as a parameter, then accomplishes the dynamic password operating process in the card.

[0039] Since the SIM card is used in the GSM system, the card can be separated from the mobile phone. One card can uniquely identify one subscriber. Therefore, at the time of loading a user dynamic password key, the dynamic password telecommunication card can use the unique identifier of the

SIM card to calculate the dynamic password key of each user with a root key, by which an effect of "one card with one password" can be achieved. Because the dynamic password telecommunication card of the user can be used in any one of GSM mobile telephones and different mobile telephones generate different dynamic passwords, the dynamic password authentication based on mobile phone is surely convenient and safety.

[0040] 3. Short Message Service Center

[0041] A short message service center provides services in an OTA mode to users of the dynamic password identity authentication system based on the mobile telephone. OTA technology (Over-the-Air technology) can have a remote management to the data and applications of the SIM card through the air interface of mobile communication (GSM or CDMA). It is the best scheme for the value-added service updating of the current 2G mobile communication network. STK (SIM card application tool kit) is a developing tool proposed in GSM11.14. The STK applies a mechanism based on a short message, which realizes a shift of a part of data service from a PC to a mobile phone and meets the requirement of the user of obtaining information in a moving state. At present, all the value added services provided by the China Mobile Communication Corporation are developed based on the STK. The "Monternet Program", which serves as a carrier of mobile internet services, can provide timely, abundant, manifold and individuated information services. In addition, because the operation of the STK services is simple and convenient, a great development has been taken. Current dynamic STK service over-the-air technology adopts advanced OTA (air interface mode) technology, by which applications in the SIM card are managed to realize a real individuated service.

[0042] OTA has the following technical advantages. The dynamic STK menu download technology takes a data short message as a carrier of information downloading. The data short message is a special short message which is not shown in a mobile telephone screen and is directly transmitted to the SIM card as data. The data is directly stored and processed by the SIM card after it is received by the card, and the transmitting and receiving of this kind of short message are only supported by the STK card.

[0043] No additional special devices are needed to be provided at mobile communication network end for using the over-the-air technology of the dynamic STK service. That is, it does not need a reconstruction of existing networks, a frequent card replacement of the users and a large investment of value added service providers, which provides a "both-win" mode for the users, operators and value added service providers.

[0044] The over-the-air technology of the dynamic STK service based on the short message can make the users download whatever they want according to their preference at any time, in any space, and it really realizes the concept of individuated service. The technology resolves the conflict between a limited card capacity and unlimited needs for value added services, and breaks through the restriction of time and space.

[0045] The "over-the-air technology of the dynamic STK service" can be applied in many circumstances using mobile electronic business, including domestic and foreign enter-

prises, banks, securities, information centers, hotels and supermarkets. The service provider can change or add contents and coding of the menu as the case may be for the choices of the users. The users can also download or update application menu timely according to their needs.

[0046] The "over-the-air technology of the dynamic STK service" can also be used to browse a dynamic menu download server of the service provider. The service provider can provide a multilevel menu on the server for the user to download, and at last one of the services can be selected by the user. The user can also select and change different service providers according to a server list provided by the mobile communication operator.

[0047] According to the present invention, an OTA mode is used to transmit data in the network by wireless communication technology. Only with clicks of the user's finger, a mobile user can transmit a dynamic password menu updating requirement towards the air menu download server by a mobile telephone. Then the server will update and amend user menu and applications in the dynamic password card in a wireless mode, by which a convenient, fast and cost effective menu download service is provided to the user.

[0048] Generally, if the user buys a dynamic password telecommunication card, all applications including the dynamic password applications are fixed. If the service provider wants to change applications in the card or provide update service to the system, in one possible way, the user should go to a designated business hall with the dynamic password telecommunication card to handle this matter. However, it is difficult for the telecommunication operator to uniformly change applications in the user card because all the cards are required to be recalled for such changing. If the OTA mode is used, the changing becomes easy. The user can apply to the telecommunication company for the contents which needs to be changed everywhere at any time. The telecommunication company can immediately send new applications to the user card after it receives the application. The telecommunication company can also change applications of all or a part of the users once by a batch sending mode.

[0049] FIG. 3 is a flowchart of the short message service center providing services in an OTA mode according to one embodiment of the present invention. As shown in FIG. 3, the operating flow of the short message service center providing services in an OTA mode is as follows:

[0050] First step: a service provider develops new services used with dynamic password application and updates timely the database of the dynamic download server.

[0051] Second step: a mobile user using the over-the-air technology of the dynamic STK service can implement a momentary query in the dynamic menu download server by a mobile telephone short message, and send timely a dynamic menu downloading request to the download server if a new service used with the dynamic password application is found, the request of the user is upload by GSM network to the SMS center (short message service center) and transmitted to the download server by a gateway;

[0052] Third step: the download server packages the dynamic menu requested by the user into a short message with a specified format, and downloads the dynamic password menu required by the user into the dynamic password

telecommunication card of the user through the primary network link in a data short message mode, which completes downloading process of the dynamic password menu and applications.

[0053] 4. Security Authentication Server

[0054] The security authentication server is the most important part of the whole system and is connected to an application system server via a local area network. It controls access to the network of all the remote users, provides all-round authentication, authorization and audit services. The security authentication server has a perfect data security self protection function in which all user data is encrypted and stored in the database, and also has safety and complete database management and backup functions. The security authentication server has a powerful graphics management interface and can provide all system management functions such as user management, operator management and audit management. The security authentication server comprises the following six parts: a system operation module, a user management module, a system communication module, a system management module, a dynamic password test module and a database.

[0055] FIG. 4 is a schematic view showing a structure of a security server according to one embodiment of the present invention. As shown in FIG. 4, the security server comprises the following parts:

System Operation Module

[0056] The system operation module uses the same dynamic password security algorithm as that in the dynamic password telecommunication card to realize verification function of the dynamic password and carefully records the operation journal. The system operation module can carry out the interconnection with the application interface.

User Management Module

[0057] The user management module has a powerful graphics management interface and can perform the delivery, delete, freezing and unfreezing of the dynamic password telecommunication card. The user management module can also carry out a query on basic information of a user of the dynamic password telecommunication card.

System Communication Module

[0058] The system communication module is connected with the system initialization module and processes the related data communications.

System Management Module

[0059] The system management module performs functions of managing each module of the system and implementing a query of the authentication journal. The system management module has a simple graphics interface to realize an all-around system management function.

Dynamic Password Telecommunication Card Test Module

[0060] The dynamic password test module is used to test in this mobile telephone whether the dynamic password telecommunication card operates properly.

Database

[0061] The database stores system information such as user information, card information, administrator informa-

tion, system settings, operating journal, in which important information (for example, user dynamic password key) is stored in an encryption mode.

[0062] II. Description of Operation Principle of the Dynamic Password Authentication System Based on the Mobile Telephone

[0063] The dynamic password telecommunication card according to the present invention is stored therein with a dynamic password security algorithm key and a dynamic password telecommunication card ID number. The dynamic password security algorithm is the 3DES algorithm which is a popular symmetrical key algorithm used worldwide. The user can have a normal mobile communication when the dynamic telecommunication card is inserted into the card slot of the mobile telephone. When the user wants to login the network information service system, a dynamic password function written in the STK menu of the card or an OTA mode can be used to download the menu into the mobile phone, after which the dynamic password function in the menu is called. At this time, the mobile telephone will prompt the user to input PIN password. If the input password is correct, the dynamic password telecommunication card will generate a dynamic password and display it in the screen of the mobile telephone.

[0064] FIG. 5 is a schematic diagram showing a dynamic password authentication system based on a mobile telephone according to the present invention.

[0065] The dynamic password telecommunication card provides the dynamic password in a time synchronism operation mode of a counter synchronism operation mode.

[0066] Time Synchronism Operation Mode

[0067] The dynamic password telecommunication card obtains time information from the mobile phone and uses a security algorithm key preset in the card to perform an encryption operation taking the time information as a parameter. Then an encryption result of an 8 or 16 bit character string is produced and displayed on the LCD of the mobile telephone.

[0068] All the information inputted by the user, including the user identity identification code and the dynamic password information, are sent to the security authentication server. The security authentication server picks up the security algorithm key of the user and the initialization time parameter of the card from the user database according to the user identity identification code, and then decrypts the received dynamic password using the security algorithm key. The decrypted time parameter is compared with the system time and a judging result of accept or deny is given considering the communication delay and the clock error.

Counter Synchronism Operation Mode

[0069] An 8 bit accumulator counter is made in the dynamic password telecommunication card. Taking the value of the counter as a parameter, the dynamic password telecommunication card uses a security algorithm key preset in the card to perform an encryption operation. Then an encryption result of an 8 bit character string is produced and displayed on the LCD of the mobile telephone. The counter will automatically plus one for each computation of the dynamic password.

[0070] All the information inputted by the user, including the user identity identification code and the dynamic password information, are sent to the security authentication server. The security authentication server picks up the security algorithm key of the user and the parameter of the previous login times from the user database according to the user identity identification code, and then decrypts the received dynamic password using the security algorithm key. The decrypted counter value is compared with the parameter of the previous login times, and a judging result of accept or deny is given considering the error caused by the denying of login.

[0071] III. Description of Operation Flow of the Dynamic Password Authentication System Based on the Mobile Telephone

[0072] A dynamic password telecommunication card is delivered to every user who wants to login the network information service system. The user can insert the dynamic password telecommunication card into the card slot of the mobile telephone to replace the telecommunication card, then a normal mobile communication can be carried out. Each time when the user login the network system via a computer to have the service, the menu can be downloaded into the mobile telephone through the STK or UTK menu written in the card or in the OTA mode, and then the dynamic password function in the menu is called. At this time, the mobile telephone prompts the user to input the PIN password of the mobile telephone. After the PIN password is verified, a dynamic password generated by the dynamic password telecommunication card is displayed on the display of the mobile telephone. The user only needs to take an 8 or 16 bit number displayed in the mobile telephone as a password of the current login and at the same time input the identity identification code of the user in the network information service system into the system through a computer keyboard, then the user can login the system.

[0073] FIG. 6 is a flowchart of the mobile telephone generating a dynamic password according to one embodiment of the present invention. FIG. 7 is a flowchart of the dynamic password authentication system authenticating a dynamic password according to the present invention. As shown in the figures, the process of the flowcharts is proceeded as follows:

[0074] A user prepares to login the system. The user takes out the mobile telephone and calls the dynamic password service item in the menu. The mobile telephone prompts the user to input the PIN password and verifies the password. After the PIN password is verified, a string of dynamic password is displayed on the LCD of the mobile telephone. The user inputs information such as the dynamic password and the identity identification code in the system through a computer keyboard at subscriber end.

[0075] All information inputted by the user, including the identity identification code and the dynamic password, are transmitted to the security authentication server. The security authentication server calls the security algorithm key of the user and initialization time parameter of the card or information of the previous login times from the user database according to the user identity identification code. The security authentication server decrypts the dynamic password transmitted from the user using the same security algorithm as the dynamic password telecommunication card

and verifies the dynamic password, and then the verification result is recorded in the system journal.

[0076] The security authentication server returns the verification result to the user and assigns the corresponding authority of the user according to the verification result, and permits the user to login the network information service system according to its authority to get corresponding information services, by which one time of authentication is carried out.

[0077] V. Description of the Distribution and Management of the Key of the Dynamic Password Telecommunication Card.

[0078] In order to realize the dynamic password authentication system based on the mobile telephone, a security algorithm key is required to be preset in the dynamic password telecommunication card of the mobile telephone. Since the mobile telephone commonly applies a symmetrical encryption algorithm in the current mobile communication, a symmetrical encryption algorithm is also used to perform the computation of the dynamic password in the present invention. In addition, the encryption and decryption key is controlled by the provider of the network information services. That is, if the provider of the network information services is a bank, then the security algorithm key is controlled by the bank; if the provider of the network information services is a government office, then the security algorithm key is controlled by the government office.

[0079] The provider of the network information services is in charge of the distribution and management of the key of the dynamic password telecommunication card.

[0080] FIG. 8 is a flowchart of a password distribution of the dynamic password telecommunication card according to one embodiment of the present invention.

[0081] The flow of the password distribution of the dynamic password telecommunication card is as follows. The provider of the network information services generates a CIC (Customer Injection Card) key through a key management system for the communication department to realize the individualization of the dynamic password telecommunication card. The provider of the network information services generates a HIC (Host Injection Card) key and uses this key in the decryption of the dynamic password information.

[0082] An authorized management center of the provider of the network information services injects the CIC key into the IC card and delivers the card to the communication department to form a master card, and at the same time provides the communication department with a control card of the card. At the time of producing the dynamic password telecommunication card of the mobile telephone, an encryption key is calculated using the CIC key and a unique identification code of the dynamic password telecommunication card and is stored in a specific area of the card, thus one card is ensured to be provided with one password.

[0083] The communication department provides the unique identification code of the individualized dynamic password telecommunication card to the provider of the network information services in a safe mode, and the dynamic password decryption module of the provider of the network information services uses the HIC key and the

unique identification code of the card to calculate the decryption key with the same algorithm. Then the decryption key which is the same as the encryption key is obtained.

[0084] HIC card is only used to download the master key into the decryption module. In order to guarantee its security, the HIC card can be used only once. After the downloading, the HIC card will be automatically disabled. The master key stored in the CIC card is consistent with that in the HIC card.

[0085] The technology improves the security of identity authentication effectively and avoids the trouble for the user to remember the password and change the password frequently. The technology is suitable to the systems that require a higher security of the identify authentication, such as the bank, the securities, the police and the electronic government affair and the like, thereby to improve the security for the system administrator and the user to register the system.

[0086] Although preferred embodiments of the present invention has been shown and described, it would be appreciated by those skilled in the art that changes may be made in these embodiments without departing from the principals and spirit of the invention, the scope of which is defined in the claims and their equivalents.

We claim:

1. A dynamic password authentication method comprising:

performing in a mobile terminal an encrypting operation using a dynamic password algorithm generating key and an initialization parameter stored in a telecommunication card to obtain an encryption result;

sending the encryption result and a user identity identification code to a security authentication server, the security authentication server seeking out the dynamic password generating algorithm key in a database based on the user identity identification code and performing a decrypting operation to the encryption result to obtain a decrypted parameter.

comparing the initialization parameter with the decrypted parameter, the mobile terminal passing the authentication if the initialization parameter is consistent with the decrypted parameter, and the authentication being denied if not.

2. The method according to claim 1, wherein the initialization parameter is time information of the mobile terminal.

3. The method according to claim 2, wherein if the time information is used as the initialization parameter, a communication delay and a clock error value are added into the decrypted parameter.

4. The method according to claim 1, wherein the initialization parameter is counting information of the mobile terminal.

5. The method according to claim 4, wherein if the counting information is used as the initialization parameter, an error value caused by the previous denying of the authentication is added.

6. The method according to claim 1, wherein the dynamic password generating algorithm key, a user menu or applications which are stored in the mobile terminal and the security authentication server are updated or changed in an Over-the-Air mode.

7. The method according to claim 6, wherein the Over-the-Air mode comprises:

a service provider updating new services used with a dynamic password in a database of a download server;

the mobile terminal implementing a momentary query to a dynamic menu download server by a mobile telephone short message, and sending a dynamic menu downloading request to the download server if new services used with the dynamic password are found, the request of the user being upload by network to the short message service center and transmitted to the download server by a gateway;

the download server packaging the dynamic menu requested by the user into a short message with a specified format, and downloading the dynamic password menu required by the user into the dynamic password telecommunication card of the user through a network link in a data short message mode.

8. The method according to claim 7, wherein the telecommunication card is a SIM card or a UIM card.

9. A dynamic password authentication system comprising:

an authentication server; and a mobile terminal connected to the authentication server via wireless communication,

the mobile terminal is provided with a dynamic password telecommunication card to generate a dynamic password,

the authentication server is stored therein with a dynamic password key corresponding to the dynamic password telecommunication card of the mobile terminal to verify the dynamic password submitted by the mobile terminal

10. The system according to claim 9, wherein it further comprises a short message service center wirelessly connected to the mobile terminal, and the short message service center provides update service for the user of the mobile terminal or the authentication server.

* * * * *



- (51) International Patent Classification:
H04W 12/06 (2009.01)
- (21) International Application Number:
PCT/EP2009/004744
- (22) International Filing Date:
1 July 2009 (01.07.2009)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
08011848.2 1 July 2008 (01.07.2008) EP
- (71) Applicant (for all designated States except US): **VODAFONE HOLDING GMBH** [DE/DE]; Mannesmannufer 2, 40213 Düsseldorf (DE).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): **MOUTARAZAK, Said** [NL/NL]; Portonnekuilstraat 18, 6163 BP Geleen (NL). **KORAICHI, Najib** [NL/NL]; Kruisstraat 38, NL-6333 CT Schimmert (NL).
- (74) Agent: **JOSTARNDT PATENTANWALTS-AG**; Brüsseler Ring 51, D-52074 Aachen (DE).
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.
- (84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GI, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM,

[Continued on next page]

(54) Title: METHOD AND DEVICE FOR GENERATING A TIME-DEPENDENT PASSWORD

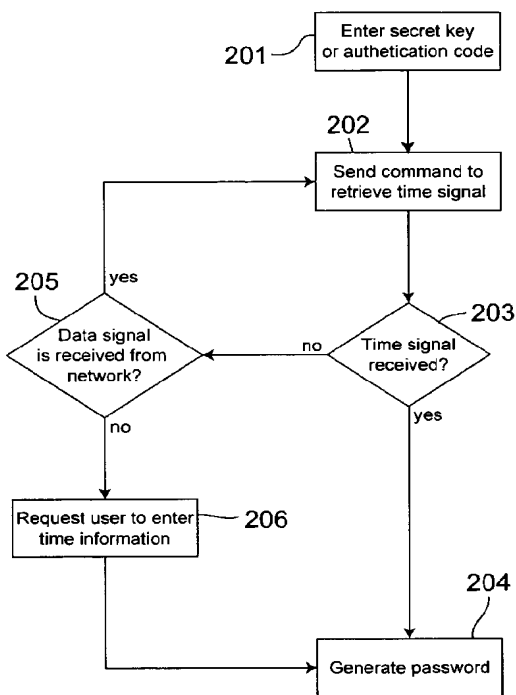


Fig. 2

(57) Abstract: The invention relates to the generation of a time-dependent password using an external time signal. For generating a time-dependent password in a temporary absence of the external time signal, the invention proposes a method comprising the steps of: - checking, whether the security device has access to an external time signal; - requesting a user of the security device to enter time information, if it is determined that the security device has no access to the external time signal; and - generating a time-dependent password using the time information entered in response to the request. The invention further relates to a device for performing the method.



WO 2010/000455 A1

TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG). **Published:**

— with international search report (Art. 21(3))

Declarations under Rule 4.17:

— of inventorship (Rule 4.17(iv))

Method and device for generating a time-dependent password

5

Technical Field

The invention relates to the generation of time-dependent passwords, particularly to the generation of time-synchronized one-time passwords. More specifically, the invention relates to a method for generating a time-dependent password in a mobile communication device. The invention further relates to a device for generating a time-dependent password in a mobile communication device and to a mobile communication device comprising the device.

15

Background of the Invention

Conventional static passwords bear the risk to be discovered by unauthorized third parties. Protection against unauthorized access to restricted resources can be improved by using so-called one-time passwords (OTPs), which are valid only for one time. An OTP mechanism, commonly referred to as time-synchronised type OTP, involves synchronised time information for generating and validating OTPs. In regular time intervals, such as, for example, every minute, a security device or an application, which is usually called "token", generates a new OTP from current time information and a secret key assigned to the user. For validating the OTP, an authorisation station re-generates the OTP based on the secret key and own current time information using the same algorithm as the token and compares the self-generated password with the password generated by the token.

In the OTP environment described before, the time information used in the token and the time information used in the authorisation station have to be well synchronised. However, in OTP environments, certain time deviations are al-

lowed, which means that the authorisation station accepts OTPs generated and based on time information that differs from that time of the authorisation station by a predefined time deviation. Typical allowed time deviations may be in the range of one or several minutes, for example.

5

The token may be a closed, tamper-resistant hardware system dedicated to the generation of OTPs, which stores the secret key of the user and which usually has a built-in clock for providing the time information. As an alternative, the token may be configured as a so-called "soft token", which is a software applica-
10 tion run on a general-purpose processor.

The international patent application WO 2007/126227 describes a mobile communication device, such as, for example, a mobile phone or a PDA (Personal Data Assistant) or the like, which has an interface for accepting an IC chip (IC: Integrated Circuit) for generating time-synchronised type OTPs. The IC chip
15 stores the user's secret key and comprises a module for generating the OTPs. The time information is provided by a base station and received by the radio frequency processing unit of the mobile communication device.

20 The IC chip allows for implementing the token for generating time-synchronised type OTPs in a mobile communication device. An external time signal provides the time information for generating the OTPs, such that a special clock for this purpose can be dispensed with. However, the time information is available only if the mobile communication device is connected to the base station. This
25 means that the generation of OTPs is not possible, if the mobile communication device cannot be connected to the base station.

Summary of the Invention

30 Therefore, it is an object of the present invention to allow for generating time-synchronised type OTPs in a device having access to an external time signal, when the device cannot receive the external time signal.

The object is achieved by a method comprising the features of claim 1 and by a device comprising the features of claim 12. Embodiments of the method and the device are given in the dependent claims.

5

According to a first aspect of the invention, a method of the type described before is proposed, which comprises the following steps:

- checking, whether the security device has access to an external time signal;
- requesting a user of the security device to enter the time information, if it is determined that the security device has no access to the external time signal; and
- generating a time-dependent password using the time information entered in response to the request.

15 According to a second aspect, the invention proposes a device for generating a time-dependent password using time information. The device comprises:

- a checking means for checking, whether an external time signal is accessible;
- a requesting means for requesting a user to enter the time information, if the checking means determines that the external time signal is not accessible, and
- a calculation means for generating a time-dependent password using the time information entered in response to the request.

25 The invention has the advantage that a time-dependent password can be generated in the absence of the external time signal. This is achieved by allowing the user of the security device to specify the time information needed for generating a time-dependent password, if no external time signal is received in the mobile communication device.

30

By allowing the user to input the time information, the invention contradicts the usual opinion that the mechanism for generating the time information needed

for calculating time-dependent passwords is a sensitive component of the password generation, which has to be secured against access by the user. Particularly, it has been discovered that the possibility to generate a time-dependent password based on the time information provided by the user is very
5 useful to bridge a temporarily absence of an external time signal.

However, if the external time signal can be received in the security device, the time signal can be used for generating the time-dependent password. This has the advantage that the risk of fraudulent misuse is reduced.
10

Therefore, in one embodiment of the method and the device, the time-dependent password is generated using the external time signal, if it is determined that the security device has access to the external time signal.

15 The time information used for generating the time-dependent password has to be synchronized with the time information used by the authorization station. However, the user may stay in a time zone different from the time zone in which the authorization station is located. If, in this case, the user entered his local time, the generated password would be invalid due to the time difference to the
20 location of the authorization station.

Therefore, in one embodiment of the method and the device, the user is requested to specify a time zone to which the entered time information refers, the time information entered by the user is converted to the time zone of an authorization station for validating the password and the time-dependent password is
25 generated using the converted time information.

In a further embodiment of the method and the device, the user is requested to enter an authentication code and the entered time information is only used for
30 generating a time-dependent password, if the authentication code has been validated successfully.

This prevents an unauthorized third party that does not dispose of the authentication code from generating a password and making fraudulent use of it. Particularly, an unauthorized third party is prevented from generating and using a password that is valid in a future point in time.

5

Furthermore, one embodiment of the method and the device comprises the steps of:

- storing the entered time information;
- determining that the security device has access to the external time signal;
- 10 - checking, whether the entered time information refers to a future point in time compared to the currently received external time signal; and
- initiating an alarm routine, if the entered time information refers to a future point in time compared to the currently received time signal.

15 This provides security against an attack based on the aforementioned generation of a password, which is valid in a future point in time.

In order to prevent an attacker from gaining unauthorized access using such a password, in one embodiment of the method and the device, the password
20 generated using the entered time information is being marked as invalid in the authorization station in response to the initiation of the alarm routine.

In a further embodiment of the method and the device, the user is requested to enter a secret key allocated to the user and the time-dependent password is
25 generated using the secret key entered by the user.

Moreover, in one embodiment of the method and the device, the generated time-dependent password is displayed at the security device and/or the time-dependent password is transmitted from the security device to the authorisation
30 station via a data network to which the security device is connected.

In one embodiment of the method, a mobile communication device comprises the security device.

5 Using a mobile communication device comprising security device for the generating the time-dependent password increases the user convenience, since a user who usually carries a mobile communication device does not need an additional device for generating the time-dependent password.

10 In one embodiment of the method and the device, the external time signal may be provided by the communication network to which the security device can be connected. Therefore, in this embodiment checking, whether the security device has access to the external time signal, comprises checking, whether the security device is connected to a communication network providing the external time signal.

15 Providing the external time signal in the communication network has the advantage that no additional equipment is needed to access the time signal, if a mobile communication device comprises the security device, since the mobile communication device usually has all components for connecting to a communication network.

20

In one embodiment of the invention, the device is a smartcard, which can be connected to a mobile communication device.

25 It is an advantage of this embodiment that the device can be provided to the user easily in the form of smartcard, which is connectable to his mobile communication device. The usage of a mobile communication device for generating the time-dependent password is especially convenient for the user due to the reasons described before. One further advantage of this embodiment is that the

30 security mechanism of the smartcard prevents fraudulent use of the device.

In mobile communication, smartcards are used for identifying and authenticating a user to a mobile communication network. Advantageously, such smartcards can also host the device according to the invention. Therefore, in one embodiment of the invention, the smartcard comprises a subscriber identification module for identifying and/or authenticating a user to a mobile communication network.

Furthermore, the invention provides a computer program comprising software code portions for performing a method of the type described before, when the computer program is run on a processor.

Moreover, the invention proposes a mobile communication device comprising a device of the type before.

These and other aspects of the invention will be apparent from and elucidated with reference to the embodiments described hereinafter making reference to the accompanying drawings.

Brief Description of the Drawings

20

In the drawings

Fig. 1 is a schematic block diagram showing a mobile communication device for generating time-synchronised type OTPs, and

25

Fig. 2 is a schematic flow chart illustrating a method for providing time information for generating the time-synchronised type OTPs.

Detailed Description of Embodiments of the Invention

30

Figure 1 shows a mobile communication device 101, which can be connected to a mobile communication network (PLMN – Public Land Mobile Network) 102,

which may be configured according to the GSM or UMTS standard, for example (GSM: Global System for Mobile communications; UMTS: Universal Mobile Telecommunications System). For connecting the mobile communication device 101 to the PLMN 102, the mobile communication device 101 comprises a radio interface 103. The radio interface 103 is coupled to a main processor 104 for controlling the operation of the mobile communication device 101. For interacting with the mobile user, the mobile communication device 101 comprises an input component 105 and a display component 106 both coupled to the main processor 104. Applications run by the main processor 104 and reference data are stored in a memory component 107 to which the main processor 104 has access.

The mobile communication device 101 interacts with a smartcard 108, which is inserted into a card reader unit 114 of the mobile communication device 101. The smartcard 108 includes a microprocessor 109 and a memory 110 and comprises a subscriber identification module allocated to the user of the mobile communication device 101. Particularly, the subscriber identification module includes information for identifying and authenticating the mobile user to the PLMN 102 and provides functionality for accessing services of the PLMN 102. The subscriber identification module may be configured in accordance with the type of the PLMN 102. If the PLMN 102 is a GSM or UMTS network, the subscriber identification module is a subscriber identity module (SIM) according to the GSM standard or a universal subscriber identity module (USIM) according to the UMTS standard.

The mobile user has the authorisation to access a restricted resource. In one embodiment, the resource may be a web application or a web service hosted by a network server 113, which is connected to a data network 112. Access to the resource is controlled by an authorisation station 111, which denies access to the resource unless the user is identified and authenticated successfully. The network server 113 may comprise the authorisation station 111, or the authorisation station 111 may reside in another network server. In the embodiment

depicted in figure 2, the network server 112 is connected to the data network 112 via the authorisation station 111. However, other network architectures are possible.

5 The authorisation station 111 performs the user authorisation using time-synchronised OTPs. This ensures a relatively high level of security of the access control. Thus, the web application may be a payment application, for example, that has to be secured efficiently against unauthorised access by third parties.

10

For generating time-synchronised OTPs, the mobile communication device 101 comprises an OTP application. The OTP application may be resident in the mobile terminal and run on the main processor 104 of the mobile communication device 101. In a different embodiment, the OTP application is resident in the smartcard 108 including the subscriber identification module. In this embodiment, the OTP application is stored in the memory 110 and run on the micro-processor 109 of the smartcard 108. This has the advantage that the OTP application is secured against unauthorised access by means of the security mechanism of the smartcard 108. In further embodiments, an OTP chip including the OTP application may be removably connected to the mobile terminal.

The mobile communication device 101 may be connected to the data network 112 via an access technology, such as, for example, a WLAN connection. In figure 1, this is schematically illustrated by means of the arrow 115. In this architecture, the mobile user may access the network server 113 using the mobile communication device 101 and OTPs generated in the mobile communication device 101 may be transmitted electronically from the mobile communication device 101 to the authorisation station 111. Furthermore, the PLMN 102 may be coupled to the data network 112, such that the mobile communication device 101 can be connected to the data network via the PLMN 102, if it is registered in the PLMN 102.

In another embodiment, the mobile user accesses the network server 113 using a further device connected to the data network 112, such as, for example, a personal computer. In this case, the OTP application outputs generated passwords at the mobile communication device 101. The user reads that generated password at the display component 106 of the mobile communication device 101 and enters the password at the device used for accessing the network server 113.

The OTP application provides a graphical user interface at the display component 106 of the mobile communication device 101 for depicting outputs to the user and for presenting input requests to the user. Moreover, the OTP application is configured to receive user inputs from the input component 105 of the mobile communication device 101. If the OTP application resides in the smartcard 108, the OTP application may access the functionalities of the mobile communication device 101 using SIM Toolkit commands, which, in general, are known to a person skilled in the art.

For generating time-synchronised OTPs, an algorithm is implemented in the OTP application, which is used to calculate OTPs based on time information and a secret key allocated to the user. The secret key may be a personal identification number (PIN), for example. The secret key may be entered by the user, when the OTP application is started or when the user requested the generation of a password. Likewise, it is possible that the secret key is stored securely in the mobile communication device 101, particularly in the smartcard 108. In this embodiment, the generation of a password may be possible only after an authorisation code entered by the user has been validated successfully by the OTP application. The authorisation code may be another PIN and differs from the secret key allocated to the user in that the secret key is used to calculate the passwords, while the authorisation code is used to unlock the password generation. Securing the OTP application with an authorisation code for unlocking the password generation has the advantage that an attacker has to use the mobile communication device 101 for generating passwords of the user, since

the secret key is secured against access within the mobile communication device 101.

For validating the password generated by the OTP application, the authorisation station 111 re-computes the passwords using the user's secret key, which is also stored in the authorisation station 111, and its own time information. The time information used by the OTP application and the time information present in the authorisation station 111 have to be synchronised accurately enough. Usually, the authorisation station 111 allows for generating passwords computed using a time information with a predetermined deviation from the time information present and authorisation station 111. For this purpose, the authorisation station 111 determines that the password is valid, if it is calculated using a time from a predetermined time interval around the current time of the authorisation station 111. The time interval may be between 1 and 15 minutes, preferably between 2 and 4 minutes.

The OTP application retrieves the time information needed for generating the time-synchronised OTPs from the PLMN 102. For this purpose, the PLMN 102 includes a supplementary service providing a time signal. The service may be accessed using so-called USSD commands (USSD: Unstructured Supplementary Service Data), which are, in general, known to a person skilled in the art in general. However, retrieving the time information from the PLMN 102 requires that the mobile communication device 101 was connected to the PLMN 102. This is not always true, since it may happen that the mobile communication device 101 is out of coverage of the PLMN 102, for example. Therefore, the OTP application requests the user to enter time information into the mobile communication device 101, in case no time information can be received from the PLMN 102.

In one embodiment, a method schematically depicted in figure 2 is implemented in the OTP application for this purpose: After the user has entered his secret key or his authorisation code in step 201, the OTP application sends a com-

mand to retrieve time information from the PLMN 102 in step 202. The command is passed to the radio interface 103 of the mobile communication device 101, which transmits the command to the PLMN 102, if the mobile communication device 101 is connected to the PLMN 102. After having passed the command to the radio interface 103 the OTP application checks, whether the command is responded within a predetermined time interval in step 203. This means that the OTP application checks, whether the time signal is received during the time interval. If the time signal is received in time, the OTP application computes a password based on the received time information and the secret key of the user in step 204.

If the OTP application determines in step 203 that no time information has been received from the PLMN 102 in the predetermined time interval, the OTP application checks, whether the mobile communication device 101 is connected to the PLMN 102 in step 205. This may be done by checking, whether the mobile communication device receives a predetermined data signal broadcasted in the PLMN 102, such as, for example, a signal identifying the PLMN 102. If it is determined in step 205 that the mobile communication device 101 is registered in the PLMN 102, the OTP application preferably goes back to step 202 and re-sends the command to retrieve the time information. However, if it is determined in step 205 that the mobile communication device 101 is not connected to the PLMN 102, the OTP application requests the user to enter time information at the mobile communication device 101. After having received the user input, the OTP application calculates a password using the time information specified by the user in step 204.

For requesting the user to input the time information, the user interface of the OTP application presented at the display component 106 of the mobile communication device may provide an input field, which may be filled in by the user using the input component 105 of the mobile communication device 101. The user may receive the time information from any available source. For example, this may be his wristwatch or a public watch in the vicinity of his position.

In order for the calculated password to be valid, the password has to be calculated using the time information present in the authorisation station 111. Particularly, this means that the time information used for the calculation should refer to the same time zone as the time information of the authorisation station 111. Therefore, in one embodiment, the user is requested to input a time information referring to the time zone of authorisation station 111 in step 206. This requires knowledge about the time zone of the authorisation station 111 and about the time shift between this time zone and the current time zone of the user.

10

In another embodiment, the user is requested to input his local time and to specify his current time zone. For the specification of the time zone, a list of the existing time zones may be presented to the user, such that the user can specify his time zone by choosing it from the list. Using the time information entered by the user and the information about the time zone the time information refers to, the OTP application calculates the local time of the authorisation station 111 and uses this calculated time to generate the password in step 204.

In order to prevent that an attacker uses the mobile communication device 101 to generate a password that will be valid in the future by inputting time information relating to a future point in time, the input of the time information by the user may be secured by an authorisation code. This means that the OTP application requests the user to enter the authorisation code besides the time information. The authorisation code is also stored securely in the mobile communication device 101, particularly in the smartcard 108. In this embodiment, the OTP application validates the authorisation code before generating a password using the time information given by the user.

Furthermore, in one embodiment, the OTP application stores at least the time information, when it calculates and outputs a password based on time information specified by the user. Particularly, the time information may be stored securely in the smartcard 108. After having stored the time information, the OTP

application monitors, whether the mobile communication device 101 connects to the PLMN 102 again. This may be done by sending commands to retrieve time information from the PLMN 102 or by checking in regular time intervals, whether a predetermined data signal broadcasted in the PLMN 102 is received in the mobile communication device 101. Again, this data signal may be a signal identifying the PLMN 102 that is broadcasted in the PLMN in regular time intervals.

If the OTP application determines that the mobile communication device 101 is connected to the PLMN 102 again, the OTP application checks, whether the time information used for calculating the password refers to a future point in time. If this is true, an alarm routine is started, since in this case an attacker might have generated the password for fraudulent use in the future. For the aforementioned check, the OTP application compares time information currently retrieved from the PLMN 102 and the stored time information. If it is determined that the stored time information referred to the future compared to the currently received time information, the OTP application starts the alarm routine.

The alarm routine may comprise informing the user that a password has been generated for a future point in time. If the user judges that the password might have been generated for fraudulent use, he may inform the authorization station 111. In another embodiment, the OTP application may inform the authorization station 111 automatically. For this purpose, the OTP application may generate a corresponding message specifying the time information in question, and the OTP application may control the mobile communication device 101 to transmit the message to the authorisation station 111. The message may be transmitted to the authorisation station 111 via the PLMN 102 or via another data connection between the mobile communication device 101 and the authorisation station 111.

After having been informed about the possible misuse, steps can be taken in the authorisation station 111 to prevent an unauthorised access to the network server 113 using the password in question. This may be done by blocking ac-

cess to the network server 113 with this password. Particularly, the password generated for the future point in time may be marked as invalid, such that this password cannot be used as an authorisation for accessing the network server 113.

5

While the invention has been illustrated and described in detail in the drawings and foregoing description, such illustration and description are to be considered illustrative or exemplary and not restrictive; the invention is not limited to the disclosed embodiments. Particularly, the invention is not limited to a download
10 of an application or program code to smartcard 106. A person skilled in the art recognises that other data can be downloaded to the smartcard 106 in the same way as it has been described before in connection with the download of a program code of an application. Other variations to the disclosed embodiments can be understood and effected by those skilled in the art in practicing the claimed
15 invention, from a study of the drawings, the disclosure, and the appended claims.

In the claims, the word "comprising" does not exclude other elements or steps, and the indefinite article "a" or "an" does not exclude a plurality. A single processor or other unit may fulfill the functions of several items recited in the claims.
20 A computer program may be stored/distributed on a suitable medium, such as an optical storage medium or a solid-state medium supplied together with or as part of other hardware, but may also be distributed in other forms, such as via the Internet or other wired or wireless telecommunication systems. Any reference
25 signs in the claims should not be construed as limiting the scope.

Claims

1. A method for generating a time-dependent password in a security device (101; 108) using time information, the method comprising the steps of:
 - checking, whether the security device has access to an external time signal;
 - requesting a user of the security device to enter the time information, if it is determined that the security device has no access to the external time signal; and
 - generating a time-dependent password using the time information entered in response to the request.
2. The method according to claim 1, wherein the time-dependent password is generated using the external time signal, if it is determined that the security device (101; 108) has access to the external time signal.
3. The method according to one of the preceding claims, wherein the user is requested to specify a time zone to which the entered time information refers, wherein the time information entered by the user is converted to the time zone of an authorization station (111) for validating the password and wherein the time-dependent password is generated using the converted time information.
4. The method according to one of the preceding claims, wherein the user is requested to enter an authentication code and wherein the entered time information is only used for generating a time-dependent password, if the authentication code has been validated successfully.
5. The method according to one of the preceding claims, further comprising the steps of:
 - storing the entered time information;
 - determining that the security device (101; 108) has access to the external time signal;

- checking, whether the entered time information refers to a future point in time compared to the currently received external time signal; and
 - initiating an alarm routine, if the entered time information refers to a future point in time compared to the currently received time signal.
6. The method according to claim 5, wherein the password generated using the entered time information is marked as invalid in the authorization station (111) in response to the initiation of the alarm routine.
 7. The method according to one of the preceding claims, wherein the user is requested to enter a secret key allocated to the user and wherein the time-dependent password is generated using the secret key entered by the user.
 8. The method according to one of the preceding claims, wherein the generated time-dependent password is displayed at the security device (101; 108) and/or wherein the time-dependent password is transmitted from the security device (101; 108) to the authorisation station (111) via a data network to which the security device (101; 108) is connected.
 9. The method according to one of the preceding claims, wherein a mobile communication device (101) comprises the security device (101; 108).
 10. The method according to one of the preceding claims, wherein checking whether the security device (101; 108) has access to the external time signal comprises checking whether the security device (101; 108) is connected to a communication network (102) providing the external time signal.
 11. A computer program comprising software code portions for performing a method according to one of the preceding claims, when the computer program is run on a processor (104; 109).

12. A device (101; 108) for generating a time dependent password using time information comprising:
- a checking means for checking, whether an external time signal is accessible;
 - a requesting means for requesting a user to enter the time information, if the checking means determines that the external time signal is not accessible, and
 - a calculation means for generating a time-dependent password using the time information entered in response to the request.
13. A device (101; 108) according claim 12, wherein the device is a smartcard (108), which can be connected to a mobile communication device (101).
14. A device according to claim 13, wherein the smartcard (108) comprises a subscriber identification module for identifying and/or authenticating a user to a mobile communication network (102).
15. A mobile communication (101) device comprising a device (101; 108) according to one of the claims 12 to 14.

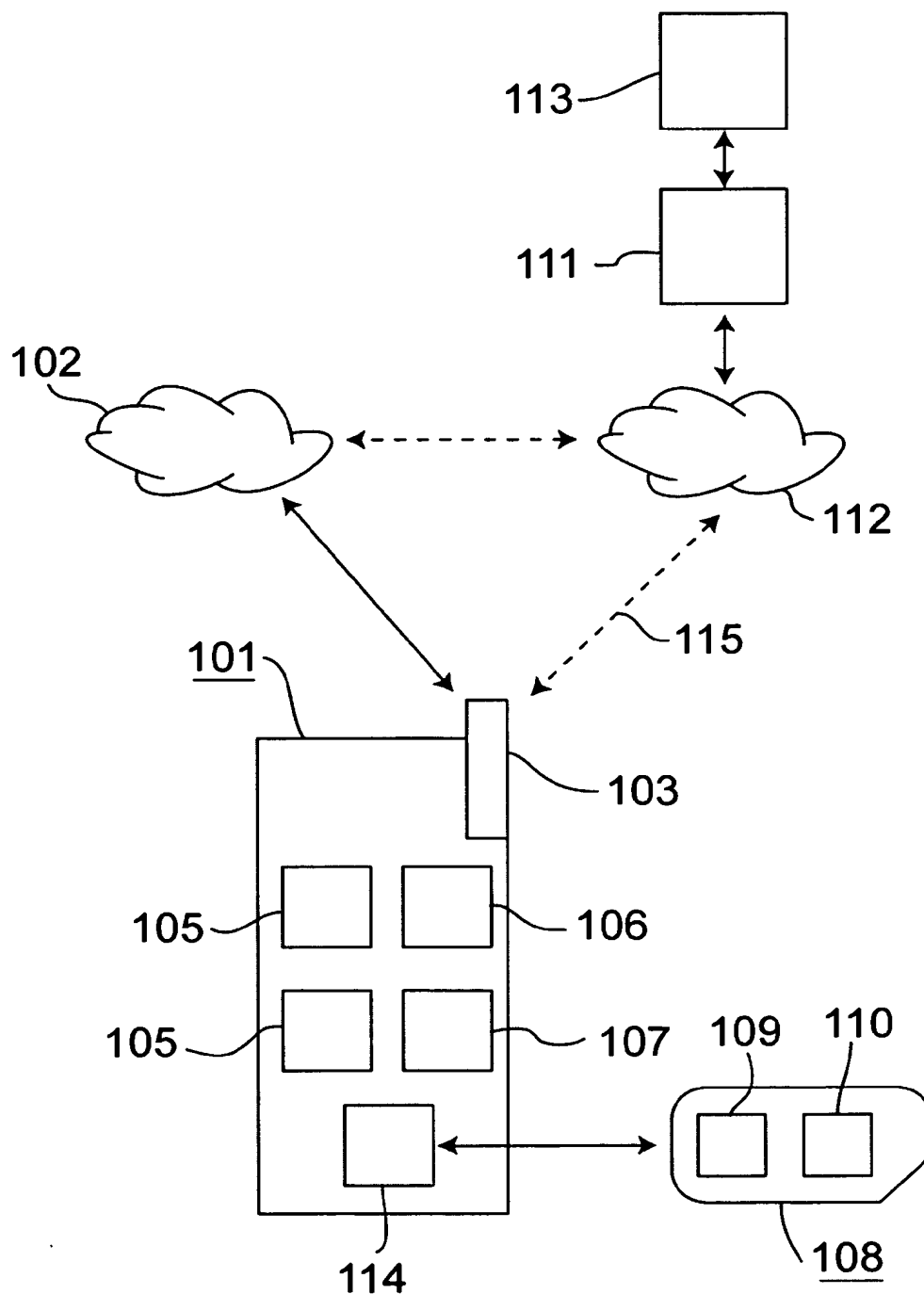


Fig. 1

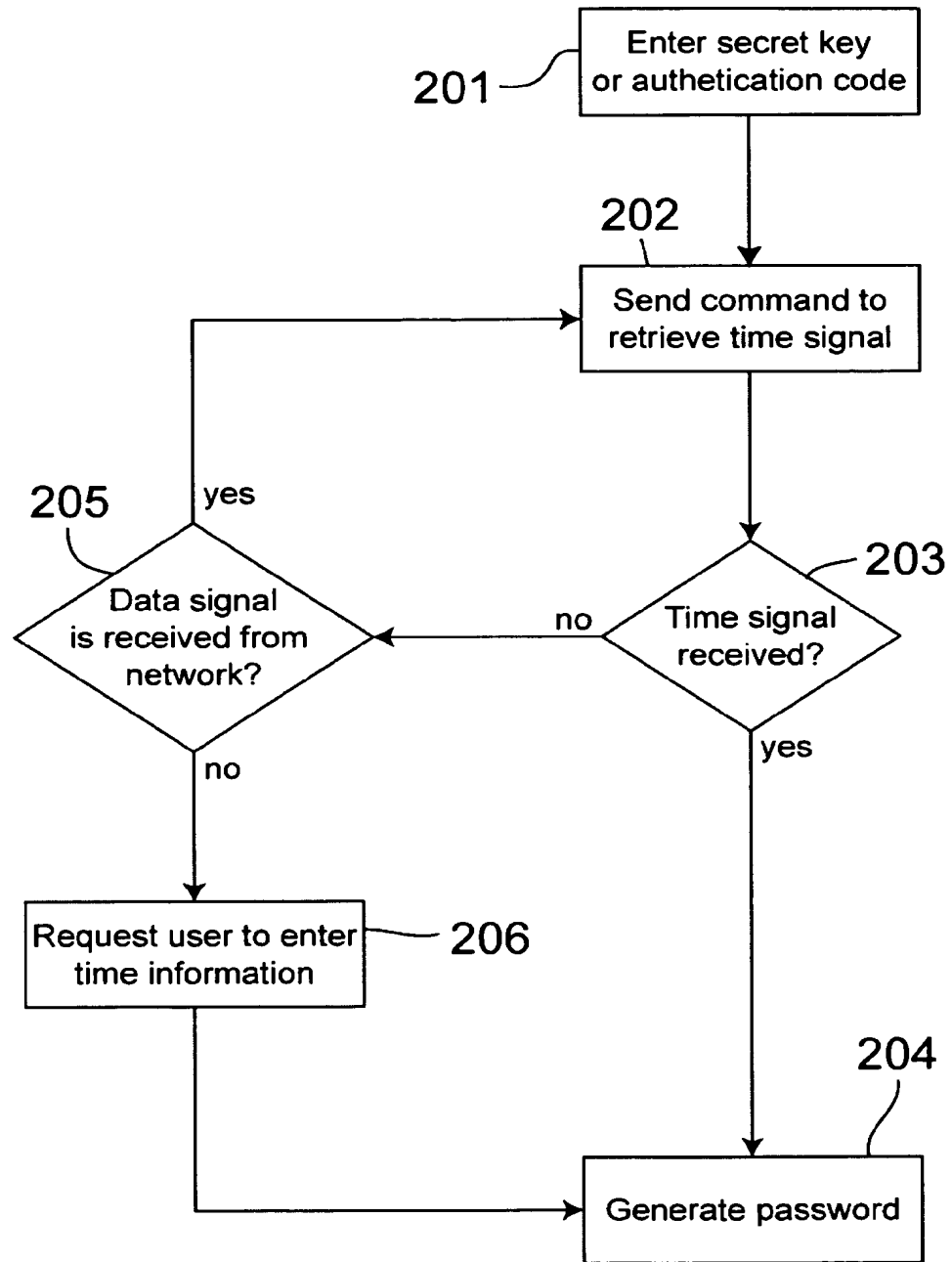


Fig. 2

INTERNATIONAL SEARCH REPORT

International application No

PCT/EP2009/004744

A. CLASSIFICATION OF SUBJECT MATTER INV. H04W12/06		
According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED		
Minimum documentation searched (classification system followed by classification symbols) H04W G06F H04L G07F		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used) EPO-Internal, WPI Data		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2007/062787 A (VODAFONE HOLDING GMBH [DE]; JUNGBLUT STEPHAN [DE]) 7 June 2007 (2007-06-07) abstract page 5, line 18 - page 6, line 27 page 14, line 27 - page 19, line 11; figures 2,3	1-15
A	EP 1 833 219 A (MONITISE LTD [GB]) 12 September 2007 (2007-09-12) paragraphs [0014] - [0018] paragraphs [0030] - [0035] paragraphs [0043], [0044]	1-15
A	US 5 226 080 A (COLE JAMES F [US] ET AL) 6 July 1993 (1993-07-06) column 2, lines 27-50 column 5, line 3 - column 6, line 36	1-15
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input checked="" type="checkbox"/> See patent family annex.		
* Special categories of cited documents : *A* document defining the general state of the art which is not considered to be of particular relevance *E* earlier document but published on or after the international filing date *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified) *O* document referring to an oral disclosure, use, exhibition or other means *P* document published prior to the international filing date but later than the priority date claimed *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art. *&* document member of the same patent family		
Date of the actual completion of the international search 25 September 2009		Date of mailing of the international search report 02/10/2009
Name and mailing address of the ISA/ European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel: (+31-70) 340-2040, Fax: (+31-70) 340-3016		Authorized officer Ruiz Sanchez, J

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/EP2009/004744

Patent document cited in search report		Publication date		Patent family member(s)		Publication date
WO 2007062787	A	07-06-2007	EP	1955515 A1		13-08-2008
EP 1833219	A	12-09-2007	WO	2007102005 A2		13-09-2007
US 5226080	A	06-07-1993	NONE			

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with 37 CFR § 1.6(a)(4).

Dated: May 20, 2013
Electronic Signature for Matthew H. Grady: /Matthew H. Grady/

Docket No.: W0537-700620
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Kenneth P. Weiss

Application No.: 11/768,729

Confirmation No.: 3536

Filed: June 26, 2007

Art Unit: 2435

For: UNIVERSAL SECURE REGISTRY

Examiner: B. W. Dada

AMENDMENT

Commissioner for Patents

Dear Madam:

INTRODUCTORY COMMENTS

In conjunction with a Request for Continued Examination and in response to the Advisory Action mailed on May 1, 2013 and the Final Office Action mailed on December 18, 2012, please amend the above-identified application as follows: Changes to the claims are shown by strike through (for deleted matter) and underlining (for added matter).

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 10 of this paper.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A secure registry system for providing information to a first party to enable transactions between the first party and entities with secure data stored in the secure registry system, the secure registry system comprising:

a database including secure data for each entity, wherein each entity is associated with a time-varying multicharacter code for each entity having secure data in the secure registry system, respectively, each time-varying multicharacter code representing an identity of one of the respective entities; and

a processor configured to receive, from the first party, at least the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed, configured to map the time-varying multicharacter code to the identity of the entity in the database using ~~only~~ the time-varying multicharacter code, to execute a restriction mechanism configured to determine compliance with any access restrictions for the first party to secure data for completing the transaction, and to allow or not allow access to secure data associated with the entity including information required to enable the transaction, the information including account identifying information, where the account identifying information is ~~unknown~~ not provided to the first party, ~~to provide~~ and the account identifying information is provided to a third party to enable the transaction with the first party and without providing the account identifying information to the first party.

2. (Canceled)

3. (Previously Presented) The system of claim 1, wherein the time-varying multicharacter code is provided to the system via a secure electronic transmission device.

4. (Previously Presented) The system of claim 1, wherein the time-varying multicharacter code is encrypted and transmitted to the system, and

wherein the system is configured to decrypt the time-varying multicharacter code with a public key of the entity.

5. (Previously Presented) The system as claimed in claim 1, wherein the transaction includes a service provided by the first party,

wherein said first party's service includes delivery,

wherein the information is an address to which an item is to be delivered to the entity,

wherein the system receives the time-varying multicharacter code, and

wherein the system uses the time-varying multicharacter code to obtain the appropriate address for delivery of the item by the third party.

6. (Canceled)

7. (Canceled)

8. (Canceled)

9. (Previously Presented) The system as claimed in claim 1, wherein the account identifying information includes credit card account information regarding the entity, and wherein the processor is configured to provide the credit card account information based upon the multicharacter code of the entity to enable the transaction.

10. (Previously Presented) The system as claimed in claim 9, wherein the system is configured to receive an approval of the credit card transaction.

11. (Previously Presented) The system as claimed in claim 1, wherein the account identifying information includes bank card account information regarding the entity, and wherein the processor is configured to provide the bank card account information to enable the transaction based upon the multicharacter code of the entity.

12. (Previously Presented) The system as claimed in claim 11, wherein the system is configured to provide an approval of the bank card transaction.
13. (Previously Presented) The system as claimed in claim 1, wherein the information includes personal identification information regarding the entity.
14. (Previously Presented) The system as claimed in claim 13, wherein the personal identification information comprises a photograph of the entity, and wherein the photograph is provided to the first party.
15. (Previously Presented) The system as claimed in claim 1, wherein the account identifying information identifies email address information regarding the entity.
16. (Currently Amended) A method for providing information to a first party to enable transactions between the first party and entities who have secure data stored in a secure registry in which each entity is identified by a time-varying multicharacter code, the method comprising:
 - receiving the time-varying multicharacter code for an entity on whose behalf a transaction is to take place;
 - mapping the time-varying multicharacter code to an identity of the entity in a database using ~~only~~ the time-varying multicharacter code;
 - determining compliance ~~based on~~ with any access restrictions for the first party to secure data for completing the transaction;
 - accessing information required to perform the transaction, the information including account identifying information ~~unknown to the first party~~;
 - providing the account identifying information to a third party without providing the account identifying information to the first party; and
 - using the account identifying information to enable the first party to perform the transaction without the first party's knowledge of the account identifying information.
17. (Canceled)

18. (Canceled)
19. (Previously Presented) The method of claim 16, wherein the act of receiving the time-varying multicharacter code comprises receiving the time-varying multicharacter code transmitted via a secure electronic transmission device.
20. (Previously Presented) The method of claim 16, wherein the act of receiving the time-varying multicharacter code comprises receiving an encrypted multicharacter code, and wherein the method further comprises decrypting the encrypted multicharacter code.
21. (Previously Presented) The method as claimed in claim 16, wherein the transaction includes a service provided by the first party,
wherein the service includes delivery,
wherein the account identifying information is associated with an address to which an item is to be delivered for the entity, and
wherein the third party receives the address for delivery of an item provided by the first party.
22. (Canceled)
23. (Canceled)
24. (Previously Presented) The method as claimed in claim 16, wherein the account identifying information includes a credit card number, and wherein the act of using the account identifying information comprises using the credit card number to enable the transaction.
25. (Previously Presented) The method as claimed in claim 24, wherein the act of using the account identifying information comprises receiving a validation or denial of the transaction without providing the credit card number of the entity to the first party.

26. (Previously Presented) The method as claimed in claim 16, wherein the act of using the account identifying information comprises using bank card information about the entity to enable a transaction.

27. (Previously Presented) The method as claimed in claim 26, wherein the act of using the information comprises receiving a validation or denial of the bank card transaction without providing a bank card number of the entity to the first party.

28. (Previously Presented) The method as claimed in claim 16, wherein the act of mapping the time-varying multicharacter code to information required by the first party comprises mapping the time-varying multicharacter code to personal identification information about the entity.

29. (Previously Presented) The method as claimed in claim 28, wherein the personal identification information comprises a photograph of the entity, and
wherein the method further comprises an act of providing the photograph to the first party.

30. (Previously Presented) The method as claimed in claim 16, wherein the account identifying information identifies email address information about the entity.

31. (Canceled).

32. (Previously Presented) The method as claimed in claim 24, further comprising an act of transmitting to the first party one of an approval or a denial of the credit card transaction.

33. (Previously Presented) The system of claim 1, wherein the database is further configured to associate biometric information with each entity having secure data in the secure registry, respectively.

34. (Previously Presented) The system of claim 33, wherein the processor is further configured to map the time-varying multicharacter code to biometric information associated with the entity on whose behalf the transaction is to be performed and to provide the biometric information to the first party.

35. (Previously Presented) The system of claim 34, wherein the biometric information includes an image of the entity on whose behalf the transaction is to be performed.

36. (Previously Presented) The system of claim 34, wherein the time-varying multicharacter code is generated by a device associated with the entity on whose behalf the transaction is to be performed.

37. (Previously Presented) The method as claimed in claim 16, further comprising an act of associating biometric information with each entity having secure data in the secure registry, respectively.

38. (Previously Presented) The method of claim 37, further comprising acts of:
mapping the time-varying multicharacter code to biometric information associated with the entity on whose behalf the transaction is to be performed; and
providing the biometric information to the first party.

39. (Previously Presented) The method of claim 38, wherein the biometric information includes an image of the entity on whose behalf the transaction is to be performed.

40. (Canceled).

41. (Previously Presented) The system of claim 1, wherein the account identifying information includes an account number.

42. (Previously Presented) The system of claim 41, wherein the account identifying information includes credit card account information and the account number includes a credit card number.

43. (Previously Presented) The system of claim 41, wherein the third party includes a financial service provider and the account number includes at least one of a debit card number and a credit card number.

44. (Previously Presented) The system of claim 43, wherein the first party includes a merchant, and the service includes a sale of at least one of goods and services.

45. (Previously Presented) The system of claim 44, wherein the processor is further configured to receive, from the first party, a merchant ID, and a purchase amount.

46. (Previously Presented) The system of claim 1, wherein the identity of the entity is unknown until the time-varying code is mapped to the identity by the processor.

47. (Currently Amended) A secure registry system for providing information to a first party to enable transactions between the first party and entities with secure data stored in the secure registry system, the secure registry system comprising:

a database including secure data for each entity, wherein each entity is associated with a time-varying multicharacter code for each entity having secure data in the secure registry system, respectively, each time-varying multicharacter code representing an identity of one of the respective entities, wherein the database is configured to permit or deny access to information on the respective entity using the time-varying multicharacter code; and

a processor configured to receive the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed, configured to map the time-varying multicharacter code to the identity of the entity to identify the entity, configured to execute a restriction mechanism ~~configured~~ to determine compliance with any access restrictions for the first party to secure data for completing the transaction, configured to obtain from the database the secure data associated with the entity including information required to enable the

transaction, the information including account identifying information, and configured to provide the account identifying information to a third party to enable the transaction without providing the account identifying information to the first party.

48. (Currently Amended) A secure registry system for providing information to a first party to enable transactions between the first party and entities with secure data stored in the secure registry system, the secure registry system comprising:

a database including secure data for each entity, wherein each entity is associated with a time-varying multicharacter code for each entity having secure data in the secure registry system, respectively, each time-varying multicharacter code representing an identity of one of the respective entities; and

a processor configured to receive the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed, configured to map the time-varying multicharacter code to the identity of the entity without requiring further information to identify the entity, configured to access from the database secure data associated with the entity including information required to enable the transaction, the information including account identifying information, and configured to provide the account identifying information to a third party to enable the transaction without providing the account identifying information to the first party, and wherein enabling the transaction without providing account identifying information to the first party includes limiting ~~the account identifying~~ transaction information provided by the secure registry system to the first party to transaction approval information.

REMARKS

Claims 1, 3-5, 9-16, 19-21, 24-30, 32-39 and 41-48 were previously pending in this application. Claims 1, 16, 47 and 48 have been amended. As a result claims 1, 3-5, 9-16, 19-21, 24-30, 32-39 and 41-48 are pending for examination with claims 1, 16, 47 and 48 being independent claims. No new matter has been added.

Advisory Action

As indicated in the Advisory Action communicated on May 1, 2013, the submitted amendments require further search and/or consideration. Applicant respectfully submits the present amendment (assuming entry of the Amendments to the claims submitted on April 12, 2013) for further considered. For the convenience of the Examiner, Applicant has included the prior argument in the April 12, 2013 Response updated to reflect the claim amendments presented herein.

Rejections Under 35 U.S.C. §103

The Office Action rejected claims 1, 3-5, 9-16, 19-21, 24-30, 32-39 and 41-48 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 7,571,139 B1 to Gioradano et al. (hereinafter Gioradano) in view of U.S. Patent No. 5,657,388 to Weiss (hereinafter Weiss). In response, Applicant has amended claims 1, 16, 47 and 48 and submits the following remarks.

Applicant respectfully asserts that the claim 1, as amended, is patentable in view of the alleged combination at least because Giordano and Weiss alone or in proper combination do not teach or suggest “a restriction mechanism configured to determine compliance with any access restrictions for the first party to secure data for completing the transaction,” as recited in claim 1, as amended.

Giordano is directed to “a network for processing retail sales transactions” including “a customer transceiver with a unique customer number” (Abstract). Giordano teaches a “transaction processing system” that processes transactions with the “appropriate payment processing center” based on received authorization requests including “the customer ID, merchant ID and transaction data” (Col. 3 Lines 29-36). In summary, Giordano teaches the use of a customer transceiver to authorize a transaction processing system to carry out a monetary transaction between a customer and a merchant at the appropriate payment processing center.

Giordano does not teach or suggest “a restriction mechanism configured to determine compliance with any access restrictions for the first party to secure data for completing the transaction,” as recited in claim 1, as amended. Rather, Giordano teaches the use of a customer transceiver to authorize a transaction processing system to carry out a monetary transaction between a customer and a merchant at the appropriate payment processing center. Accordingly, claim 1, as amended, distinguishes over the Giordano reference.

Weiss is directed to “a method and apparatus for utilizing a token” to “provide secure access by authorized users to a selected resource” (Abstract). Weiss teaches the generation and use of a one-time variable multi-character code based in part on information stored in the token to authenticate the user’s identity. Weiss does not teach or suggest “a restriction mechanism configured to determine compliance with any access restrictions for the first party to secure data for completing the transaction,” as recited in claim 1, as amended. Rather, Weiss teaches the use of a one-time variable multi-character code based in part on information stored in a user’s token to authenticate a user. Accordingly, claim 1, as amended, distinguishes over the Weiss reference.

As neither Giordano nor Weiss teach or suggest “a restriction mechanism configured to determine compliance with any access restrictions for the first party to secure data for completing the transaction,” the combination, even if assumed proper, does not teach or suggest claim 1, as amended. Claims 3-5, 9-15, 33-36 and 41-46 depend from claim 1 and are allowable for at least the same reasons. Accordingly, withdrawal of the rejection of claims 1, 3-5, 9-15, 33-36 and 41-46 under 35 U.S.C. §103(a) is respectfully requested.

Independent Claim 16

Independent claim 16, as amended, recites “determining compliance with any access restrictions for the first party to secure data for completing the transaction.” As discussed above with respect to claim 1, Giordano teaches the use of a customer transceiver to authorize a transaction processing system to carry out a monetary transaction between a customer and a merchant at the appropriate payment processing center. Thus, Giordano does teach or suggest “determining compliance with any access restrictions for the first party to secure data for completing the transaction,” as recited in claim 16, as amended. Assuming the combination is proper, the addition of Weiss does not cure this deficiency as Weiss does not teach or suggest

“determining compliance with any access restrictions for the first party to secure data for completing the transaction,” as recited in claim 16, as amended. Claims 19-21, 24-30, 32 and 37-39 depend from claim 16 and are allowable for at least the same reasons. Accordingly, withdrawal of the rejection of claims 16, 19-21, 24-30, 32 and 37-39 under 35 U.S.C. §103(a) is respectfully requested.

Independent Claim 47

Independent claim 47 is also patentable in view of the alleged combination at least because Giordano and Weiss alone or in proper combination do not teach or suggest “restriction mechanism to determine compliance with any access restrictions for the first party to secure data for completing the transaction,” as recited in claim 47, as amended. As discussed above with respect to claim 1, Giordano teaches the use of a customer transceiver to authorize a transaction processing system to carry out a monetary transaction between a customer and a merchant at the appropriate payment processing center. The addition of Weiss does not cure this deficiency. Accordingly, withdrawal of the rejection of claim 47 under 35 U.S.C. §103(a) is respectfully requested.

Independent Claim 48

Independent claim 48, as amended, is patentable in view of the alleged combination at least because Giordano and Weiss alone or in proper combination do not teach or suggest “wherein enabling the transaction without providing account identifying information to the first party includes limiting transaction information provided by the secure registry system to the first party to transaction approval information,” as recited claim 48, as amended. Giordano teaches the “transaction processing system” transmitting to the online merchant “identification information and other data unique to the associated customer in the absence of a retail transaction” (See Col. 4 Lines 17-21). Giordano explicitly teaches the transmission of information regarding the user (e.g., entity or purchaser), including loyalty program information (See e.g., Col. 4 Lines 54-58), to a merchant (e.g., first party) rather than limiting the information transmitted to the merchant to transaction approval information. Accordingly, Giordano does not teach or suggest claim 48, as amended. Assuming the combination is proper, the addition of Weiss does not cure this deficiency. Weiss teaches the use of a one-time variable

multi-character code based in part on information stored in a user's token to authenticate a user. Thus, Weiss does not teach "wherein enabling the transaction without providing account identifying information to the first party includes limiting the account identifying information provided by the secure registry system to the first party to transaction approval information," as recited in claim 48, as amended. Accordingly, withdrawal of the rejection of claim 48 under 35 U.S.C. §103(a) is respectfully requested.

CONCLUSION

In view of the foregoing amendments and remarks, reconsideration is respectfully requested. This application should now be in condition for allowance; a notice to this effect is respectfully requested. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicant's attorney at the telephone number listed below.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee that is not covered by an accompanying payment, please charge any deficiency to Deposit Account No. 50/2762 (W0537-700620).

Dated: May 20, 2013

Respectfully submitted,

Electronic signature: /Matthew H. Grady/
Matthew H. Grady

Registration No.: 52,957

John N. Anastasi

Registration No.: 37,765

LANDO & ANASTASI LLP

Riverfront Office Park

One Main Street

Suite 1100

Cambridge, Massachusetts 02142

(617) 395-7000

Attorney for Applicant

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		11768729
	Filing Date		2007-06-26
	First Named Inventor	Kenneth P. Weiss	
	Art Unit		2435
	Examiner Name	B. W. Dada	
	Attorney Docket Number		W0537-700620

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6498861		2002-12-24	Hamid et al.	
	2	7237117		2007-06-26	Weiss	
	3	5457747		1995-10-10	Drexler et al.	
	4	6950521		2005-09-27	Marcovici et al.	
	5	8001055		2011-08-16	Weiss	
	6	7809651		2010-10-05	Weiss	
	7	7805372		2010-09-28	Weiss	
	8	8234220		2012-07-31	Weiss	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	11768729
Filing Date	2007-06-26
First Named Inventor	Kenneth P. Weiss
Art Unit	2435
Examiner Name	B. W. Dada
Attorney Docket Number	W0537-700620

9	7766223		2010-08-03	Mello et al.	
---	---------	--	------------	--------------	--

If you wish to add additional U.S. Patent citation information please click the Add button. [Add](#)

U.S.PATENT APPLICATION PUBLICATIONS

[Remove](#)

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	20030229637	A1	2003-12-11	Baxter et al.	
	2	20030046540	A1	2003-03-06	Nakamura et al.	
	3	20020184538		2002-12-05	Sugimura et al.	
	4	20030028481		2003-02-06	Flitcroft et al.	
	5	20030084332		2003-05-01	Krasinski et al.	
	6	20030085808		2003-05-08	Goldberg	
	7	20050113070		2005-05-26	Okabe	
	8	20050238147		2005-10-27	Carro	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	11768729
Filing Date	2007-06-26
First Named Inventor	Kenneth P. Weiss
Art Unit	2435
Examiner Name	B. W. Dada
Attorney Docket Number	W0537-700620

9	20070256120		2007-11-01	Shatzkamer et al.	
10	20090292641		2009-11-26	Weiss	
11	20100000455		2010-01-07	Harper	
12	20110258120		2011-10-20	Weiss	
13	20130024374		2013-01-24	Weiss	
14	20120037479		2012-02-16	Lucchi et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. **Add**

FOREIGN PATENT DOCUMENTS

Remove

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² i	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	2010000455	WO	A1	2010-01-07	Vodafone Holding Gmbh et al.		<input type="checkbox"/>

If you wish to add additional Foreign Patent Document citation information please click the Add button **Add**

NON-PATENT LITERATURE DOCUMENTS

Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		11768729
	Filing Date		2007-06-26
	First Named Inventor	Kenneth P. Weiss	
	Art Unit		2435
	Examiner Name	B. W. Dada	
	Attorney Docket Number		W0537-700620

1	"Biometrics: Who's Watching You?", Electronic Frontier Foundation (EFF), September 2003, all pages, http://www.eff.org/wp/biometrics-whos-watching-you .	<input type="checkbox"/>
2	"PGP: An introduction to cryptography", 2000, all pages.	<input type="checkbox"/>
3	"Single Sign On Authentication", Authentication World, March 13, 2007, all pages, retrieved July 9, 2010 via Wayback Machine, < http://web.archive.org/web/20070313200434/http://www.authenticationworld.com/Single-Sign-On-Authentication/ >.	<input type="checkbox"/>
4	HUNGTINGTON, "101 Things to know about single sign on", Authentication World, 2006, all pages, < http://www.authenticationworld.com/Single-Sign-On-Authentication/101ThingsToKnowAboutSingleSignOn.pdf >.	<input type="checkbox"/>
5	KESSLER, "An overview of cryptography", August 22, 2002, all pages, retrieved via Wayback Machine on January 19, 2010, http://www.garykessler.net/library/crypto.html .	<input type="checkbox"/>
6	Treasury Board of Canada Secretariat, PKI for Beginners Glossary, http://www.tbs-sct.gc.ca/pki-icp/beginners/glossary-eng.asp	<input type="checkbox"/>
7	"Bluetooth Technology FAQ", Mobileinfo.com, 21 January 2001, all pages, http://www.web.archive.org/web/200101211551/http://www.mobileinfo.com/Bluetooth/FAQ.htm	<input type="checkbox"/>
8	International Search Report and Written Opinion for International Application No. PCT/US2011/051966, 49 pages (2012).	<input type="checkbox"/>

If you wish to add additional non-patent literature document citation information please click the Add button Add

EXAMINER SIGNATURE

Examiner Signature	Date Considered
--------------------	-----------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	11768729
Filing Date	2007-06-26
First Named Inventor	Kenneth P. Weiss
Art Unit	2435
Examiner Name	B. W. Dada
Attorney Docket Number	W0537-700620

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

- See attached certification statement.
- The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.
- A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Matthew H. Grady/	Date (YYYY-MM-DD)	2013-05-20
Name/Print	Matthew H. Grady	Registration Number	52957

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Patent Application Fee Transmittal

Application Number:	11768729
Filing Date:	26-Jun-2007
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Filer:	Matthew H. Grady
Attorney Docket Number:	W0537-700620

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Extension - 2 months with \$0 paid	2252	1	300	300

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
RCE - 2nd and Subsequent Request	2820	1	850	850
Total in USD (\$)				1150

Electronic Acknowledgement Receipt

EFS ID:	15820024
Application Number:	11768729
International Application Number:	
Confirmation Number:	3536
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Customer Number:	37462
Filer:	Matthew H. Grady
Filer Authorized By:	
Attorney Docket Number:	W0537-700620
Receipt Date:	20-MAY-2013
Filing Date:	26-JUN-2007
Time Stamp:	18:25:04
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$1150
RAM confirmation Number	6140
Deposit Account	502762
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	Request_for_Continued_Examination_Fillable_PDF_2.PDF	697706	no	3
			fd5d783e1158b7641f5e1f3cd0d2878b57bfcd9		
Warnings:					
Information:					
2	Transmittal Letter	Information_Disclosure_State_ment_3.pdf	23145	no	2
			44854b7d97b954491026398b4f1d1c229060b79e		
Warnings:					
Information:					
3	Non Patent Literature	Biometrics_4.PDF	1188833	no	12
			2a958db2c8dc9302e16d333e603550da84ed57f8		
Warnings:					
Information:					
4	Non Patent Literature	PGP_5.PDF	4369745	no	86
			e33d119bd6fcc15b6819408a49349a316ee7e9b0		
Warnings:					
Information:					
5	Non Patent Literature	SingleSign_6.PDF	123555	no	2
			e0a62da1fe36f5b03eb325dd518e207bcb4b2bf		
Warnings:					
Information:					
6	Non Patent Literature	Huntington_101_7.PDF	261178	no	5
			d97fc98756e9b3531d6b0fbd9324246db49622		
Warnings:					
Information:					
7	Non Patent Literature	Kessler_8.PDF	4769737	no	63
			15a0bf9849773d41fd9a4e0d1a04971d2ff9141b		
Warnings:					
Information:					
8	Non Patent Literature	A_Glossary_Of_Common_PKI_Terms_9.PDF	177844	no	4
			33d635b8e78b3382f2091b28e0e7a69059776435		
Warnings:					

Information:					
9	Non Patent Literature	Bluetooth_FAQ_10.PDF	269582 f3a3730ff18c7a13d57a6ac46f081e8a70d8b15c	no	4
Warnings:					
Information:					
10	Non Patent Literature	PCTUS2011051966_ISR_11.PDF	2277133 2353d95108cdb2eecb88a16a1d41674693395bd8	no	49
Warnings:					
Information:					
11	Foreign Reference	WO2010000455A1_13.PDF	955186 dbb8350bcf2cd9490bd394dbc34891b08a5etcd	no	24
Warnings:					
Information:					
12		AAAamendmentwithRCE.pdf	3081557 f3996e3d9e7976fa2636fc245ff1055311ef7d54	yes	13
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Amendment Submitted/Entered with Filing of CPA/RCE		1	1	
	Claims		2	9	
Applicant Arguments/Remarks Made in an Amendment		10	13		
Warnings:					
Information:					
13	Information Disclosure Statement (IDS) Form (SB08)	IDSfillable.pdf	613655 82dd8e144f74dccc8785b711035ab7ebaef3aef3	no	6
Warnings:					
Information:					
14	Fee Worksheet (SB06)	fee-info.pdf	31992 a8ee992a1ec2834b41f5eac55487309748588b2e	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			18840848		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Electronic Acknowledgement Receipt

EFS ID:	15820024
Application Number:	11768729
International Application Number:	
Confirmation Number:	3536
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Customer Number:	37462
Filer:	Matthew H. Grady
Filer Authorized By:	
Attorney Docket Number:	W0537-700620
Receipt Date:	20-MAY-2013
Filing Date:	26-JUN-2007
Time Stamp:	18:25:04
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$1150
RAM confirmation Number	6140
Deposit Account	502762
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Request for Continued Examination (RCE)	Request_for_Continued_Examination_Fillable_PDF_2.PDF	697706	no	3
			fd5d783e1158b7641f5e1f3cd0d2878b57bfcd9		
Warnings:					
Information:					
2	Transmittal Letter	Information_Disclosure_State ment_3.pdf	23145	no	2
			44854b7d97b954491026398b4f1d1c229060b79e		
Warnings:					
Information:					
3	Non Patent Literature	Biometrics_4.PDF	1188833	no	12
			2a958db2c8dc9302e16d333e603550da84ed57f8		
Warnings:					
Information:					
4	Non Patent Literature	PGP_5.PDF	4369745	no	86
			e33d119bd6fcc15b6819408a49349a316ee7e9b0		
Warnings:					
Information:					
5	Non Patent Literature	SingleSign_6.PDF	123555	no	2
			e0a62da1fe36f5b03eb325dd518e207bcb4b2bf		
Warnings:					
Information:					
6	Non Patent Literature	Huntington_101_7.PDF	261178	no	5
			d97fc98756e9b3531d6b0fbd9324246db49622		
Warnings:					
Information:					
7	Non Patent Literature	Kessler_8.PDF	4769737	no	63
			15a0bf9849773d41fd9a4e0d1a04971d2ff9141b		
Warnings:					
Information:					
8	Non Patent Literature	A_Glossary_Of_Common_PKI_Terms_9.PDF	177844	no	4
			33d635b8e78b3382f2091b28e0e7a69059776435		
Warnings:					

Information:					
9	Non Patent Literature	Bluetooth_FAQ_10.PDF	269582 f3a3730ff18c7a13d57a6ac46f081e8a70d8b15c	no	4
Warnings:					
Information:					
10	Non Patent Literature	PCTUS2011051966_ISR_11.PDF	2277133 2353d95108cdb2eecb88a16a1d41674693395bd8	no	49
Warnings:					
Information:					
11	Foreign Reference	WO2010000455A1_13.PDF	955186 dbb8350bcf2cd9490bd394dbc34891b08a5etcd	no	24
Warnings:					
Information:					
12		AAAamendmentwithRCE.pdf	3081557 f3996e3d9e7976fa2636fc245ff1055311ef7d54	yes	13
	Multipart Description/PDF files in .zip description				
	Document Description		Start	End	
	Amendment Submitted/Entered with Filing of CPA/RCE		1	1	
	Claims		2	9	
Applicant Arguments/Remarks Made in an Amendment		10	13		
Warnings:					
Information:					
13	Information Disclosure Statement (IDS) Form (SB08)	IDSfillable.pdf	613655 82dd8e144f74dccc8785b711035ab7ebaef3aef3	no	6
Warnings:					
Information:					
14	Fee Worksheet (SB06)	fee-info.pdf	31992 a8ee992a1ec2834b41f5eac55487309748588b2e	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			18840848		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 11/768,729	Filing Date 06/26/2007	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

ENTITY: LARGE SMALL MICRO

APPLICATION AS FILED – PART I

FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)
<input type="checkbox"/> BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>	N/A	N/A	N/A	
<input type="checkbox"/> SEARCH FEE <small>(37 CFR 1.16(k), (l), or (m))</small>	N/A	N/A	N/A	
<input type="checkbox"/> EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A	N/A	
TOTAL CLAIMS <small>(37 CFR 1.16(i))</small>	minus 20 =	*	X \$ =	
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>	minus 3 =	*	X \$ =	
<input type="checkbox"/> APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.16(j))</small>				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

	(Column 1)	(Column 2)	(Column 3)	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)
AMENDMENT	05/20/2013	CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR		
	Total <small>(37 CFR 1.16(i))</small>	* 38	Minus	** 38	= 0	X \$40 = 0
	Independent <small>(37 CFR 1.16(h))</small>	* 4	Minus	***4	= 0	X \$210 = 0
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>					
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>					
					TOTAL ADD'L FEE	0

	(Column 1)	(Column 2)	(Column 3)	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT		HIGHEST NUMBER PREVIOUSLY PAID FOR		
	Total <small>(37 CFR 1.16(i))</small>	*	Minus	**	=	X \$ =
	Independent <small>(37 CFR 1.16(h))</small>	*	Minus	***	=	X \$ =
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>					
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>					
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
 ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
 *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
 The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
 /VIKKI GRAY/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/768,729	06/26/2007	Kenneth P. Weiss	W0537-700620	3536
37462	7590	10/02/2013	EXAMINER	
LANDO & ANASTASI, LLP ONE MAIN STREET, SUITE 1100 CAMBRIDGE, MA 02142			GYORFI, THOMAS A	
			ART UNIT	PAPER NUMBER
			2435	
			NOTIFICATION DATE	DELIVERY MODE
			10/02/2013	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@LALaw.com
gengelso@LALaw.com

DETAILED ACTION

1. Claims 1, 3-5, 9-16, 19-21, 24-30, 32-39, & 41-48 remain for examination. The amendment filed 5/20/13 amended claims 1, 16, 47, & 48.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 5/20/13 has been entered.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on 5/20/13 was filed after the mailing date of the Final Rejection on 12/18/12. The submission is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Response to Arguments

4. Applicant's arguments, see pages 10-13 of the amendment filed 5/20/13, with respect to the rejection(s) of claim(s) 1-48 under 35 USC 103(a) have been fully considered and are persuasive. Therefore, the rejection has been withdrawn.

Art Unit: 2435

However, upon further search and consideration of the art, a new ground(s) of rejection is made in view of the newly discovered reference U.S. Patent 7,742,967 (hereinafter, "Keresman").

Claim Objections

5. Applicant is advised that should claim 1 be found allowable, claim 47 will be objected to under 37 CFR 1.75 as being a substantial duplicate thereof. When two claims in an application are duplicates or else are so close in content that they both cover the same thing, despite a slight difference in wording, it is proper after allowing one claim to object to the other as being a substantial duplicate of the allowed claim. See MPEP § 706.03(k).

Claim Rejections - 35 USC § 103

6. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

7. Claims 1, 3-5, 9-16, 19-21, 24-30, 32-39, & 41-48 are rejected under pre-AIA 35 U.S.C. 103(a) as being unpatentable over Giordano (U.S. Patent 7,571,139) in view of Keresman (U.S. Patent 7,742,967).

Regarding claims 1, 47, and 48:

Giordano teaches a secure registry system comprising: a database including secure data for each entity, wherein each entity is associated with a [*time-varying*] multi-

Art Unit: 2435

character code for each entity having secure data in the secure registry system, respectively, each [*time-varying*] multi-character code representing an identity of one of the respective entities (col. 18, lines 14-47); and a processor configured to receive, from the first party, at least the [*time-varying*] multi-character code for the entity on whose behalf a transaction is to be performed, configured to map the [*time-varying*] multi-character code to the identity of the entity in the database using the [*time-varying*] multi-character code, and to allow or not allow access to secure data associated with the entity including information required to enable the transaction, the information including account identifying information, wherein the account identifying information is not provided to the first party, and the account identifying information is provided to a third party to enable the transaction with the first party and without providing the account identifying information to the first party (i.e. note that the POS system does not get access to customers credit/debit account information: col. 18, lines 5-47). Specific to claim 48, Giordano further discloses wherein enabling the transaction without providing the account identifying information to the first party includes limiting transaction information provided by the secure registry system to the first party to transaction approval information (the buyer either succeeds in purchasing his desired products or is declined, with no other information being provided: col. 18, line 65 – col. 19, line 15).

Giordano does not disclose wherein his multi-character code is a time-varying multi-character code; nor [specific to claims 1 & 47] does Giordano disclose a restriction mechanism configured to determine compliance with any access restrictions for the first party to secure data for completing the transaction. However, Keserman discloses a

Art Unit: 2435

related invention for securing e-commerce wherein in addition to explicitly disclosing the use of time-varying multi-character codes for identity verification and authentication (col. 7, lines 1-45), but additionally Keserman discloses wherein his invention comprises a restriction mechanism that can specify and enforce access restrictions for the first party to secure data for completing the transaction (i.e. even if the first party can successfully authenticate oneself to the system, said first party may be restricted to where, when and with whom one may conduct transactions with: col. 6, lines 45-65). It would have been obvious to incorporate these features of Keserman's e-commerce system into Giordano's, as time-varying multi-character codes have long since been known in the art as an obvious improvement for authentication (e.g. Keserman, col. 7, lines 35-45), while the restriction mechanism provides the obvious benefits of protecting customers from transactions with dubious merchants, or preventing one from spending beyond one's approved limits (col. 6, lines 60-65).

Regarding claim 16:

Giordano discloses a method comprising: receiving the [*time-varying*] multi-character code for an entity on whose behalf a transaction is to take place (col. 18, lines 15-20); mapping the [*time-varying*] multi-character code to an identity of the entity in a database using the [*time-varying*] multi-character code (col. 18, lines 20-35); accessing information required to perform the transaction, the information including account identifying information (col. 18, lines 20-54); providing the account identifying information to a third party without providing the account identifying information to the

Art Unit: 2435

first party (i.e. note that the POS system does not get access to customers credit/debit account information: col. 18, lines 5-47); and using the account identifying information to enable the first party to perform the transaction without the first party's knowledge of the account identifying information (Ibid).

Giordano does not disclose wherein his multi-character code is a time-varying multi-character code; nor does Giordano disclose determining compliance with any access restrictions for the first party to secure data for completing the transaction. However, Keserman discloses a related invention for securing e-commerce wherein in addition to explicitly disclosing the use of time-varying multi-character codes for identity verification and authentication (col. 7, lines 1-45), but additionally Keserman discloses wherein his invention comprises a restriction mechanism that can specify and enforce access restrictions for the first party to secure data for completing the transaction (i.e. even if the first party can successfully authenticate oneself to the system, said first party may be restricted to where, when and with whom one may conduct transactions with: col. 6, lines 45-65). It would have been obvious to incorporate these features of Keserman's e-commerce system into Giordano's, as time-varying multi-character codes have long since been known in the art as an obvious improvement for authentication (e.g. Keserman, col. 7, lines 35-45), while the restriction mechanism provides the obvious benefits of protecting customers from transactions with dubious merchants, or preventing one from spending beyond one's approved limits (col. 6, lines 60-65).

Regarding claims 3 and 19:

The combination further discloses wherein the multi-character code is provided to the system via a secure electronic transmission device (Giordano: col. 18, lines 14-47; Keresman: col. 7, lines 1-35).

Regarding claims 4 and 20:

The combination further discloses wherein the code is encrypted and transmitted to the system and wherein the system is configured to decrypt the code with a public key of the entity (Giordano: col. 18, lines 14-47).

Regarding claims 5 and 21:

The combination further discloses wherein said service provider includes delivery, wherein the information is an address to which an item is to be delivered to the entity, wherein the system receives the code and wherein the system uses the code to obtain the appropriate address for delivery of the item by the third party (Giordano: *ibid*; Keresman: col. 9, lines 15-30).

Regarding claims 9 and 24:

The combination further discloses wherein the account identifying information includes a credit card number, and wherein the act of using the account identifying

Art Unit: 2435

information comprises using the credit card number to enable the transaction (Giordano: col. 16, lines 45-67; Keresman: col. 11, lines 30-50).

Regarding claims 10 and 25:

The combination further discloses wherein the act of using the account identifying information comprises receiving a validation or denial of the transaction without providing the credit card number of the entity to the first party (Ibid).

Regarding claims 11 and 26:

The combination further discloses wherein the account identifying information includes bank card account information regarding the entity, and wherein the processor is configured to provide the bank card account information to enable the transaction based upon the multi-character code of the entity (Giordano: col. 16, lines 45-67; Keresman, col. 11, lines 30-50; debit cards equally applicable at col. 10, lines 28-45).

Regarding claims 12 and 27:

The combination further discloses wherein the system is configured to provide an approval of the bank card transaction without providing a bank card number of the entity to the first party (Giordano: col. 18, lines 40-67; Keresman: col. 10, lines 28-45).

Regarding claims 13 and 28:

Art Unit: 2435

The combination further discloses wherein the information includes personal identification information regarding the entity (Giordano: col. 16, lines 30-40; Keresman: col. 4, lines 40-55).

Regarding claims 14 and 29:

The combination further discloses wherein the personal identification comprises a photograph of the entity, and wherein the photograph is provided to the first party (Giordano: picture ID at col. 11, lines 35-45).

Regarding claims 15 and 30:

The combination further discloses wherein the account identifying information identifies email address information regarding the entity (Keresman: col. 4, lines 40-60).

Regarding claim 32:

The combination further discloses an act of transmitting to the first party one of an approval or denial of the credit card transaction (Giordano: col. 18, line 65 – col. 19, line 15; Keresman: col. 6, lines 5-20).

Regarding claims 33 and 37:

The combination further discloses wherein the database is further configured to associate biometric information with each entity having secure data in the secure registry, respectively (Keresman: col. 8, lines 35-46).

Regarding claims 34 and 38:

The combination further discloses wherein the processor is further configured to map the time-varying multi-character code to biometric information associated with the entity on whose behalf the transaction is to be performed and to provide the biometric information to the first party (Keresman: col. 8, lines 10-45).

Regarding claims 35 and 39:

The combination further discloses wherein the biometric information includes an image of the entity on whose behalf the transaction is to be performed (Keresman: Ibid; see also Giordano: col. 11, lines 35-45).

Regarding claim 36:

The combination further discloses wherein the time-varying multi-character code is generated by a device associated with the entity on whose behalf the transaction is to be performed (the credit token: Keresman: col. 7, lines 1-20).

Regarding claim 41:

The combination further discloses wherein the account identifying information includes an account number (Giordano: col. 18, lines 15-20; Keresman: col. 5, lines 40-60).

Art Unit: 2435

Regarding claim 42:

The combination further discloses wherein the account identifying information includes credit card account information and the account number includes a credit card number (Giordano: col. 9, lines 10-20; Keresman: col. 6, lines 5-25).

Regarding claim 43:

The combination further discloses wherein the third party includes a financial service provider and the account number includes at least one of a debit card number and a credit card number (Giordano: Ibid; Keresman: Ibid).

Regarding claim 44:

The combination further discloses wherein the first party includes a merchant, and the service includes a sale of at least one of goods and services (Giordano: col. 9, lines 45-60; Keresman: col. 4, lines 40-60).

Regarding claim 45:

The combination further discloses wherein the processor is further configured to receive, from the first party, a merchant ID, and a purchase amount (Giordano: col. 10, lines 25-35; Keresman: col. 10, line 45 – col. 11, line 30).

Regarding claim 46:

Art Unit: 2435

The combination further discloses wherein the identity of the entity is unknown until the time-varying code is mapped to the identity by the processor (Giordano: col. 18, lines 5-47).

Conclusion

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas Gyorfi whose telephone number is (571)272-3849. The examiner can normally be reached on 10:00am - 6:30pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Hirl can be reached on (571) 272-3685. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Application/Control Number: 11/768,729

Page 13

Art Unit: 2435

/Thomas Gyorfi/
Examiner, Art Unit 2435
9/25/13

/Darren B Schwartz/
Primary Examiner, Art Unit 2435

Notice of References Cited	Application/Control No. 11/768,729	Applicant(s)/Patent Under Reexamination WEISS, KENNETH P.	
	Examiner Thomas Gyorfi	Art Unit 2435	Page 1 of 1

U.S. PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A US-7,742,967	06-2010	Keresman et al.	705/37
	B US-			
	C US-			
	D US-			
	E US-			
	F US-			
	G US-			
	H US-			
	I US-			
	J US-			
	K US-			
	L US-			
	M US-			


FOREIGN PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N				
	O				
	P				
	Q				
	R				
	S				
	T				

NON-PATENT DOCUMENTS

*	Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)				
	U				
	V				
	W				
	X				

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims 	Application/Control No. 11768729	Applicant(s)/Patent Under Reexamination WEISS, KENNETH P.
	Examiner BEEMNET W DADA	Art Unit 2435

✓	Rejected
=	Allowed


-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

Claims renumbered in the same order as presented by applicant
 CPA
 T.D.
 R.1.47

CLAIM		DATE							
Final	Original	07/16/2009	09/25/2013						
	1	✓	✓						
	2	✓	-						
	3	✓	✓						
	4	✓	✓						
	5	✓	✓						
	6	✓	-						
	7	✓	-						
	8	✓	-						
	9	✓	✓						
	10	✓	✓						
	11	✓	✓						
	12	✓	✓						
	13	✓	✓						
	14	✓	✓						
	15	✓	✓						
	16	✓	✓						
	17	✓	-						
	18	✓	-						
	19	✓	✓						
	20	✓	✓						
	21	✓	✓						
	22	✓	-						
	23	✓	-						
	24	✓	✓						
	25	✓	✓						
	26	✓	✓						
	27	✓	✓						
	28	✓	✓						
	29	✓	✓						
	30	✓	✓						
	31		-						
	32		✓						
	33		✓						
	34		✓						
	35		✓						
	36		✓						

<i>Index of Claims</i> 	Application/Control No. 11768729	Applicant(s)/Patent Under Reexamination WEISS, KENNETH P.
	Examiner BEEMNET W DADA	Art Unit 2435

✓	Rejected
=	Allowed

-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

Claims renumbered in the same order as presented by applicant
 CPA
 T.D.
 R.1.47

CLAIM		DATE							
Final	Original	07/16/2009	09/25/2013						
	37		✓						
	38		✓						
	39		✓						
	40		-						
	41		✓						
	42		✓						
	43		✓						
	44		✓						
	45		✓						
	46		✓						
	47		✓						
	48		✓						

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S1	3	((("6018724") or ("7571139") or ("5657388")).PN.	US-PGPUB; USPAT	OR	OFF	2013/08/22 17:35
S2	8	US-6498861-\$.DID. OR US-7237117-\$.DID. OR US-5457747-\$.DID. OR US-6950521-\$.DID. OR US-8001055-\$.DID. OR US-7809651-\$.DID. OR US-7805372-\$.DID. OR US-8234220-\$.DID.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/08/23 15:40
S3	9	US-7766223-\$.DID. OR US-20030229637-\$.DID. OR US-20030046540-\$.DID. OR US-20020184538-\$.DID. OR US-20030028481-\$.DID. OR US-20030084332-\$.DID. OR US-20030085808-\$.DID. OR US-20050113070-\$.DID. OR US-20050238147-\$.DID.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/08/23 15:41
S4	6	US-20070256120-\$.DID. OR US-20090292641-\$.DID. OR US-20100000455-\$.DID. OR US-20110258120-\$.DID. OR US-20130024374-\$.DID. OR US-20120037479-\$.DID.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/08/23 15:42
S5	254	"5657388".uref.	US-PGPUB; USPAT	OR	OFF	2013/09/25 16:30
S6	27	S5 and @ad<"20010316"	US-PGPUB; USPAT	OR	OFF	2013/09/25 16:31
S7	11	S6 and restrict\$3	US-PGPUB; USPAT	OR	OFF	2013/09/25 16:37
S8	1390	713/169.ccls.	US-PGPUB; USPAT	OR	OFF	2013/09/25 16:56
S9	3037	713/182.ccls.	US-PGPUB; USPAT	OR	OFF	2013/09/25 16:57
S10	917	713/184.ccls.	US-PGPUB; USPAT	OR	OFF	2013/09/25 16:57
S11	0	707/9.ccls.	US-PGPUB; USPAT	OR	OFF	2013/09/25 16:57
S12	2927	707/999.009.ccls.	US-PGPUB; USPAT	OR	OFF	2013/09/25 16:58
S13	1634	(S8 S9 S10 S12) and @ad<"20010316"	US-PGPUB; USPAT	OR	OFF	2013/09/25 16:58
S14	318	S13 and (token timecode (time near2 code))	US-PGPUB;	OR	OFF	2013/09/25 16:59

			USPAT			
S15	152	S14 and restrict\$3	US- PGPUB; USPAT	OR	OFF	2013/09/25 16:59

EAST Search History (Interference)

< This search history is empty >

9/25/2013 6:38:42 PM

C:\Users\tgyorfi\Documents\EAST\Workspaces\11768729.wsp

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		11768729
	Filing Date		2007-06-26
	First Named Inventor	Kenneth P. Weiss	
	Art Unit		2435
	Examiner Name	B. W. Dada	
	Attorney Docket Number		W0537-700620

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	6498861		2002-12-24	Hamid et al.	
	2	7237117		2007-06-26	Weiss	
	3	5457747		1995-10-10	Drexler et al.	
	4	6950521		2005-09-27	Marcovici et al.	
	5	8001055		2011-08-16	Weiss	
	6	7809651		2010-10-05	Weiss	
	7	7805372		2010-09-28	Weiss	
	8	8234220		2012-07-31	Weiss	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	11768729
Filing Date	2007-06-26
First Named Inventor	Kenneth P. Weiss
Art Unit	2435
Examiner Name	B. W. Dada
Attorney Docket Number	W0537-700620

9	7766223		2010-08-03	Mello et al.	
---	---------	--	------------	--------------	--

If you wish to add additional U.S. Patent citation information please click the Add button.

[Add](#)

U.S.PATENT APPLICATION PUBLICATIONS

[Remove](#)

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	20030229637	A1	2003-12-11	Baxter et al.	
	2	20030046540	A1	2003-03-06	Nakamura et al.	
	3	20020184538		2002-12-05	Sugimura et al.	
	4	20030028481		2003-02-06	Flitcroft et al.	
	5	20030084332		2003-05-01	Krasinski et al.	
	6	20030085808		2003-05-08	Goldberg	
	7	20050113070		2005-05-26	Okabe	
	8	20050238147		2005-10-27	Carro	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	11768729
Filing Date	2007-06-26
First Named Inventor	Kenneth P. Weiss
Art Unit	2435
Examiner Name	B. W. Dada
Attorney Docket Number	W0537-700620

9	20070256120		2007-11-01	Shatzkamer et al.	
10	20090292641		2009-11-26	Weiss	
11	20100000455		2010-01-07	Harper	
12	20110258120		2011-10-20	Weiss	
13	20130024374		2013-01-24	Weiss	
14	20120037479		2012-02-16	Lucchi et al.	

If you wish to add additional U.S. Published Application citation information please click the Add button. **Add**

FOREIGN PATENT DOCUMENTS

Remove

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² i	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	2010000455	WO	A1	2010-01-07	Vodafone Holding Gmbh et al.		<input type="checkbox"/>

If you wish to add additional Foreign Patent Document citation information please click the Add button **Add**

NON-PATENT LITERATURE DOCUMENTS

Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		11768729	
Filing Date		2007-06-26	
First Named Inventor	Kenneth P. Weiss		
Art Unit	2435		
Examiner Name	B. W. Dada		
Attorney Docket Number	W0537-700620		

1	"Biometrics: Who's Watching You?", Electronic Frontier Foundation (EFF), September 2003, all pages, http://www.eff.org/wp/biometrics-whos-watching-you .	<input type="checkbox"/>
2	"PGP: An introduction to cryptography", 2000, all pages.	<input type="checkbox"/>
3	"Single Sign On Authentication", Authentication World, March 13, 2007, all pages, retrieved July 9, 2010 via Wayback Machine, < http://web.archive.org/web/20070313200434/http://www.authenticationworld.com/Single-Sign-On-Authentication/ >.	<input type="checkbox"/>
4	HUNGTINGTON, "101 Things to know about single sign on", Authentication World, 2006, all pages, < http://www.authenticationworld.com/Single-Sign-On-Authentication/101ThingsToKnowAboutSingleSignOn.pdf >.	<input type="checkbox"/>
5	KESSLER, "An overview of cryptography", August 22, 2002, all pages, retrieved via Wayback Machine on January 19, 2010, http://www.garykessler.net/library/crypto.html .	<input type="checkbox"/>
6	Treasury Board of Canada Secretariat, PKI for Beginners Glossary, http://www.tbs-sct.gc.ca/pki-icp/beginners/glossary-eng.asp	<input type="checkbox"/>
7	"Bluetooth Technology FAQ", Mobileinfo.com, 21 January 2001, all pages, http://www.web.archive.org/web/200101211551/http://www.mobileinfo.com/Bluetooth/FAQ.htm	<input type="checkbox"/>
8	International Search Report and Written Opinion for International Application No. PCT/US2011/051966, 49 pages (2012).	<input type="checkbox"/>

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature	/Thomas Gyorfii/	Date Considered	08/23/2013
--------------------	------------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	11768729		
Filing Date	2007-06-26		
First Named Inventor	Kenneth P. Weiss		
Art Unit	2435		
Examiner Name	B. W. Dada		
Attorney Docket Number	W0537-700620		

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Matthew H. Grady/	Date (YYYY-MM-DD)	2013-05-20
Name/Print	Matthew H. Grady	Registration Number	52957

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**


Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /TG/

Search Notes 	Application/Control No. 11768729	Applicant(s)/Patent Under Reexamination WEISS, KENNETH P.
	Examiner BEEMNET W DADA	Art Unit 2435

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
713	169, 182, 184	12/10/2012	BD
707	9	12/10/2012	BD
713	169, 182, 184	9/25/13	TAG
707	9	9/25/13	TAG

SEARCH NOTES		
Search Notes	Date	Examiner
East search	12/10/2012	BD
NPL search	12/10/2012	BD
Inventor name search	12/10/2012	BD
EAST search (updated)	9/25/13	TAG

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

--	--

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with 37 CFR § 1.6(a)(4).

Dated: January 2, 2013
Electronic Signature for Marcus E. Browne: / Marcus E. Browne /

Docket No.: W0537-700620
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Kenneth P. Weiss

Application No.: 11/768,729

Confirmation No.: 3536

Filed: June 26, 2007

Art Unit: 2435

For: UNIVERSAL SECURE REGISTRY

Examiner: Thomas A. Gyorfi

AMENDMENT IN RESPONSE TO NON-FINAL OFFICE ACTION UNDER 37 C.F.R. 1.111

Commissioner for Patents

Dear Madam:

INTRODUCTORY COMMENTS

In response to the Office Action dated October 2, 2013, please amend the above-identified U.S. patent application as follows:

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 11 of this paper.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A secure registry system for providing information to a first party to enable transactions between the first party and entities with secure data stored in the secure registry system, the secure registry system comprising:

a database including secure data for each entity, wherein each entity is associated with a time-varying multicharacter code for each entity having secure data in the secure registry system, respectively, each time-varying multicharacter code representing an identity of one of the respective entities; and

a processor configured to receive, ~~from the first party,~~ a transaction request including at least the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed and an indication of the first party requesting the transaction, configured to map the time-varying multicharacter code to the identity of the entity in the database using the time-varying multicharacter code, to execute a restriction mechanism configured to determine compliance with any access restrictions for the first party to secure data for completing the transaction based at least in part on the indication of the first party and the time-varying multicharacter code of the transaction request, and to allow or not allow access to the secure data associated with the entity including information required to enable the transaction based on the determined compliance with any access restrictions for the first party, the information including account identifying information, wherein ~~where~~ the account identifying information is not provided to the first party and the account identifying information is provided to a third party to enable or deny the transaction with the first party ~~and~~ without providing the account identifying information to the first party.

2. (Canceled)

3. (Previously Presented) The system of claim 1, wherein the time-varying multicharacter code is provided to the system via a secure electronic transmission device.

4. (Previously Presented) The system of claim 1, wherein the time-varying multicharacter code is encrypted and transmitted to the system, and

wherein the system is configured to decrypt the time-varying multicharacter code with a public key of the entity.

5. (Previously Presented) The system as claimed in claim 1, wherein the transaction includes a service provided by the first party,

wherein said first party's service includes delivery,

wherein the information is an address to which an item is to be delivered to the entity,

wherein the system receives the time-varying multicharacter code, and

wherein the system uses the time-varying multicharacter code to obtain the appropriate address for delivery of the item by the third party.

6. – 8. (Canceled)

9. (Previously Presented) The system as claimed in claim 1, wherein the account identifying information includes credit card account information regarding the entity, and wherein the processor is configured to provide the credit card account information based upon the multicharacter code of the entity to enable the transaction.

10. (Previously Presented) The system as claimed in claim 9, wherein the system is configured to receive an approval of the credit card transaction.

11. (Previously Presented) The system as claimed in claim 1, wherein the account identifying information includes bank card account information regarding the entity, and wherein the processor

is configured to provide the bank card account information to enable the transaction based upon the multicharacter code of the entity.

12. (Previously Presented) The system as claimed in claim 11, wherein the system is configured to provide an approval of the bank card transaction.

13. (Previously Presented) The system as claimed in claim 1, wherein the information includes personal identification information regarding the entity.

14. (Previously Presented) The system as claimed in claim 13, wherein the personal identification information comprises a photograph of the entity, and wherein the photograph is provided to the first party.

15. (Previously Presented) The system as claimed in claim 1, wherein the account identifying information identifies email address information regarding the entity.

16. (Currently Amended) A method for providing information to a first party to enable transactions between the first party and entities who have secure data stored in a secure registry in which each entity is identified by a time-varying multicharacter code, the method comprising:

receiving a transaction request including at least the time-varying multicharacter code for an entity on whose behalf a transaction is to take place and an indication of the first party requesting the transaction;

mapping the time-varying multicharacter code to an identity of the entity in a database using the time-varying multicharacter code;

determining compliance with any access restrictions for the first party to secure data for completing the transaction based at least in part on the indication of the first party and the time-varying multicharacter code of the transaction request;

accessing information required to perform the transaction based on the determined compliance with any access restrictions for the first party, the information including account identifying information;

providing the account identifying information to a third party without providing the account identifying information to the first party to enable or deny the transaction; and

~~using the account identifying information to enable~~ enabling or denying the first party to perform the transaction without the first party's knowledge of the account identifying information.

17. – 18. (Canceled)

19. (Previously Presented) The method of claim 16, wherein the act of receiving the time-varying multicharacter code comprises receiving the time-varying multicharacter code transmitted via a secure electronic transmission device.

20. (Previously Presented) The method of claim 16, wherein the act of receiving the time-varying multicharacter code comprises receiving an encrypted multicharacter code, and wherein the method further comprises decrypting the encrypted multicharacter code.

21. (Previously Presented) The method as claimed in claim 16, wherein the transaction includes a service provided by the first party,
wherein the service includes delivery,
wherein the account identifying information is associated with an address to which an item is to be delivered for the entity, and
wherein the third party receives the address for delivery of an item provided by the first party.

22. – 23. (Canceled)

24. (Previously Presented) The method as claimed in claim 16, wherein the account identifying information includes a credit card number, and wherein the act of using the account identifying information comprises using the credit card number to enable the transaction.

25. (Previously Presented) The method as claimed in claim 24, wherein the act of using the account identifying information comprises receiving a validation or denial of the transaction without providing the credit card number of the entity to the first party.

26. (Previously Presented) The method as claimed in claim 16, wherein the act of using the account identifying information comprises using bank card information about the entity to enable a transaction.

27. (Previously Presented) The method as claimed in claim 26, wherein the act of using the information comprises receiving a validation or denial of the bank card transaction without providing a bank card number of the entity to the first party.

28. (Previously Presented) The method as claimed in claim 16, wherein the act of mapping the time-varying multicharacter code to information required by the first party comprises mapping the time-varying multicharacter code to personal identification information about the entity.

29. (Previously Presented) The method as claimed in claim 28, wherein the personal identification information comprises a photograph of the entity, and
wherein the method further comprises an act of providing the photograph to the first party.

30. (Previously Presented) The method as claimed in claim 16, wherein the account identifying information identifies email address information about the entity.

31. (Canceled)

32. (Previously Presented) The method as claimed in claim 24, further comprising an act of transmitting to the first party one of an approval or a denial of the credit card transaction.

33. (Previously Presented) The system of claim 1, wherein the database is further configured to associate biometric information with each entity having secure data in the secure registry, respectively.

34. (Previously Presented) The system of claim 33, wherein the processor is further configured to map the time-varying multicharacter code to biometric information associated with the entity on whose behalf the transaction is to be performed and to provide the biometric information to the first party.

35. (Previously Presented) The system of claim 34, wherein the biometric information includes an image of the entity on whose behalf the transaction is to be performed.

36. (Previously Presented) The system of claim 34, wherein the time-varying multicharacter code is generated by a device associated with the entity on whose behalf the transaction is to be performed.

37. (Previously Presented) The method as claimed in claim 16, further comprising an act of associating biometric information with each entity having secure data in the secure registry, respectively.

38. (Previously Presented) The method of claim 37, further comprising acts of:
mapping the time-varying multicharacter code to biometric information associated with the entity on whose behalf the transaction is to be performed; and
providing the biometric information to the first party.

39. (Previously Presented) The method of claim 38, wherein the biometric information includes an image of the entity on whose behalf the transaction is to be performed.

40. (Canceled)

41. (Previously Presented) The system of claim 1, wherein the account identifying information includes an account number.

42. (Previously Presented) The system of claim 41, wherein the account identifying information includes credit card account information and the account number includes a credit card number.

43. (Previously Presented) The system of claim 41, wherein the third party includes a financial service provider and the account number includes at least one of a debit card number and a credit card number.

44. (Previously Presented) The system of claim 43, wherein the first party includes a merchant, and the service includes a sale of at least one of goods and services.

45. (Previously Presented) The system of claim 44, wherein the processor is further configured to receive, from the first party, a merchant ID, and a purchase amount.

46. (Previously Presented) The system of claim 1, wherein the identity of the entity is unknown until the time-varying code is mapped to the identity by the processor.

47. (Currently Amended) A secure registry system for providing information to a first party to enable transactions between the first party and entities with secure data stored in the secure registry system, the secure registry system comprising:

a database including secure data for each entity, wherein each entity is associated with a time-varying multicharacter code for each entity having secure data in the secure registry system,

respectively, each time-varying multicharacter code representing an identity of one of the respective entities, wherein the database is configured to permit or deny access to information on the respective entity using the time-varying multicharacter code; and

a processor configured to receive the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed, configured to map the time-varying multicharacter code to the identity of the entity to identify the entity, configured to execute a restriction mechanism to determine compliance with any access restrictions for the first party to at least one portion of secure data for completing the transaction and to store an appropriate code with each such portion of secure data, configured to obtain from the database the secure data associated with the entity including information required to enable the transaction, the information including account identifying information, and configured to provide the account identifying information to a third party to enable or deny the transaction without providing the account identifying information to the first party.

48. (Previously Presented) A secure registry system for providing information to a first party to enable transactions between the first party and entities with secure data stored in the secure registry system, the secure registry system comprising:

a database including secure data for each entity, wherein each entity is associated with a time-varying multicharacter code for each entity having secure data in the secure registry system, respectively, each time-varying multicharacter code representing an identity of one of the respective entities; and

a processor configured to receive the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed, configured to map the time-varying multicharacter code to the identity of the entity without requiring further information to identify the entity, configured to access from the database secure data associated with the entity including information required to enable the transaction, the information including account identifying information, and configured to provide the account identifying information to a third party to enable or deny the transaction without providing the account identifying information to the first party, and wherein enabling or denying the transaction without providing account identifying information to the first

party includes limiting transaction information provided by the secure registry system to the first party to transaction approval information.

REMARKS

Claims 1, 3-5, 9-16, 19-21, 24-30, 32-39, and 41-48 were previously pending in this application. Claims 1, 16, 44, and 47 have been amended. As a result claims 1, 3-5, 9-16, 19-21, 24-30, 32-39, and 41-48 are pending for examination with claims 1, 16, 47 and 48 being independent claims. No new matter has been added.

Claim Objections

The Office Action object to claim 47 as allegedly being a substantial duplicate of claim 1. Without acceding to the correctness of this objection, Applicant has amended claims 1 and 47 to overcome this objection. Accordingly, withdrawal of the objection to claim 47 is respectfully requested.

Rejections Under 35 U.S.C. §103

The Office Action rejected claims 1, 3-5, 9-16, 19-21, 24-30, 32-39, and 41-48 under 35 U.S.C. §103(a) as being unpatentable over U.S. Patent No. 7,571,139 to Giordano (hereinafter “Giordano”) in view of U.S. Patent No. 7,742,967 to Keresman (hereinafter “Keresman”). Without acceding to the substance of this rejection, Applicant has amended independent claims 1, 16, and 47 to further clarify the distinctions between the claims as pending and the asserted combination of references and submits the following remarks.

Claim 1, as amended, is directed to “a secure registry system for providing information to a first party to enable transactions between the first party and entities with secure data stored in the secure registry system.” The system comprises “a processor configured to receive a transaction request” that includes “the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed and an indication of the first party requesting the transaction” and “execute[s] a restriction mechanism configured to determine compliance with any access restrictions for the first party to secure data for completing the transaction ***based at least in part on the indication of the first party and the time-varying multicharacter code of the transaction request,***” as recited in claim 1, as amended.

Giordano is directed to “a network for processing retail sales transactions” including “a customer transceiver with a unique customer number” (Abstract). Giordano teaches a “transaction processing system” that processes transactions with the “appropriate payment processing center” based on received authorization requests including “the customer ID, merchant ID and transaction data” (Col. 3 Lines 29-36). In summary, Giordano teaches the use of a customer transceiver to authorize a transaction processing system to carry out a monetary transaction between a customer and a merchant at the appropriate payment processing center.

Claim 1, as amended, is patentable over Giordano because Giordano does not teach or suggest “a restriction mechanism configured to determine compliance with any access restrictions for the first party to secure data for completing the transaction *based at least in part on the indication of the first party and the time-varying multicharacter code of the transaction request.*” Rather, Giordano teaches the use of a customer transceiver to authorize a transaction processing system to carry out a monetary transaction between a customer and a merchant at the appropriate payment processing center. Thus, Giordano does not teach or suggest “a restriction mechanism configured to determine compliance with any access restrictions for the first party to secure data for completing the transaction *based at least in part on the indication of the first party and the time-varying multicharacter code of the transaction request,*” as recited in claim 1, as amended. Accordingly, claim 1, as amended, distinguishes over the Giordano reference.

Keresman is directed to “a method of processing commercial transactions carried out over the Internet” where the commercial transactions are “between account holders” and “participating merchants” (Abstract). Keresman teaches that the “account holder record” may “contain information or data relating to account privileges” that may be “customize[d] or modif[ied]” (Col. 6 Lines 44-49). The account privileges may “restrict the account so that purchases thereon are not authorized for specific participating merchants or sellers,” restrict “automatically reoccurring transactions,” or restrict “single purchases over a certain price” (Col. 6 Lines 54-64). In summary, Keresman teaches the storage of account holder records that may limit specific types of transactions.

Applicant respectfully asserts that the addition of Keresman to Giordano does not cure the deficiencies discussed above with regard to Giordano. In particular, Keresman does not teach or suggest “a restriction mechanism configured to determine compliance with any access restrictions

for the first party to secure data for completing the transaction ***based at least in part on the indication of the first party and the time-varying multicharacter code of the transaction request,***” as recited in claim 1, as amended. Rather, Keresman simply discloses the storage of account holder records that may limit specific types of transactions. Therefore, Keresman does not teach or suggest a restriction mechanism that uses a “time-varying multicharacter code” in combination with an “indication of the first party” to “determine compliance with any access restrictions,” as recited in claim 1. Accordingly, claim 1, as amended, distinguishes over the Keresman reference.

As neither Giordano nor Keresman teach or suggest at least one element of claim 1, the combination, even if assumed proper, does not teach or suggest claim 1, as amended. Claims 3-5, 9-15, 33-36 and 41-46 depend from claim 1 and are allowable for at least the same reasons. Accordingly, withdrawal of the rejection of claims 1, 3-5, 9-15, 33-36 and 41-46 under 35 U.S.C. §103(a) is respectfully requested.

Independent Claim 16

Independent claim 16, as amended, is directed to “a method for providing information to a first party to enable transactions between the first party and entities who have secure data stored in a secure registry in which each entity is identified by a time-varying multicharacter code.” The method includes, inter alia, “receiving a transaction request including at least the time-varying multicharacter code for an entity on whose behalf a transaction is to take place and an indication of the first party requesting the transaction” and “determining compliance with any access restrictions for the first party to secure data for completing the transaction ***based at least in part on the indication of the first party and the time-varying multicharacter code of the transaction request,***” as recited in claim 16, as amended. As discussed above with respect to claim 1, Giordano teaches the use of a customer transceiver to authorize a transaction processing system to carry out a monetary transaction between a customer and a merchant at the appropriate payment processing center. Thus, Giordano does teach or suggest “determining compliance with any access restrictions for the first party to secure data for completing the transaction ***based at least in part on the indication of the first party and the time-varying multicharacter code of the transaction request,***” as recited in claim 16, as amended. Assuming without admitting that the combination is proper, the

addition of Keresman does not cure this deficiency. Claims 19-21, 24-30, 32 and 37-39 depend from claim 16 and are allowable for at least the same reasons. Accordingly, withdrawal of the rejection of claims 16, 19-21, 24-30, 32, and 37-39 under 35 U.S.C. §103(a) is respectfully requested.

Independent Claim 47

Independent claim 47 is directed to “a secure registry system for providing information to a first party to enable transactions between the first party and entities with secure data stored in the secure registry system.” The system comprises “a processor configured to receive the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed” and “execute a restriction mechanism to *determine compliance with any access restrictions for the first party to at least one portion of secure data for completing the transaction* and to *store an appropriate code with each such portion of secure data*,” as recited in claim 47. As discussed above with respect to claim 1, Giordano teaches the use of a customer transceiver to authorize a transaction processing system to carry out a monetary transaction between a customer and a merchant at the appropriate payment processing center. Thus, Giordano does not teach or suggest “a restriction mechanism to *determine compliance with any access restrictions for the first party to at least one portion of secure data for completing the transaction* and to *store an appropriate code with each such portion of secure data*,” as recited in claim 47. Assuming without admitting that the combination is proper, the addition of Keresman does not cure this deficiency. Accordingly, withdrawal of the rejection of claim 47 under 35 U.S.C. §103(a) is respectfully requested.

Independent Claim 48

Independent claim 48 is directed to “a secure registry system for providing information to a first party to enable transactions between the first party and entities with secure data stored in the secure registry system.” The system comprises “a processor configured to receive the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed” and “provide the account identifying information to a third party to enable or deny the transaction without providing the account identifying information to the first party” wherein “enabling or denying the

transaction without providing account identifying information to the first party includes ***limiting transaction information provided by the secure registry system to the first party to transaction approval information***,” as recited in claim 48. In contrast, Giordano teaches the “transaction processing system” transmitting to the online merchant “identification information and other data unique to the associated customer in the absence of a retail transaction” (See Col. 4 Lines 17-21). Giordano explicitly teaches the transmission of information regarding the user (e.g., entity or purchaser), including loyalty program information (See e.g., Col. 4 Lines 54-58), to a merchant (e.g., first party) rather than limiting the information transmitted to the merchant to transaction approval information. The Office Action alleges on page 4 that Giordano discloses that “the buyer either succeeds in purchasing his desired products or is declined, with no other information being provided: col. 18, line 65 – col. 19, line 15.” However, the section cited in the Office Action (i.e., col. 18, line 65 – col. 19, line 15) of Giordano explicitly states that “authorization ***and the award data*** (if any) are transmitted to the merchant” (Col. 18 Lines 64-65). Further, Giordano states that even when “the transaction does not require authorization,” the “transaction processing system” still provides “transaction information ***and loyalty program information***” (Col. 19 Lines 19-24). Accordingly, Giordano does not teach or suggest claim 48, as amended. Assuming without admitting that the combination is proper, the addition of Keresman does not cure this deficiency. Accordingly, withdrawal of the rejection of claim 48 under 35 U.S.C. §103(a) is respectfully requested.

CONCLUSION

In view of the foregoing amendments and remarks, reconsideration is respectfully requested. This application should now be in condition for allowance; a notice to this effect is respectfully requested. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicant's attorney at the telephone number listed below.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee that is not covered by an accompanying payment, please charge any deficiency to Deposit Account No. 50/2762 (Ref. No. W0537-700620).

Dated: January 2, 2013

Respectfully submitted,

Electronic signature: / Marcus E. Browne /
Marcus E. Browne
Registration No.: 71,891
Matthew H. Grady
Registration No.: 52,957
LANDO & ANASTASI LLP
Riverfront Office Park
One Main Street
Suite 1100
Cambridge, Massachusetts 02142
(617) 395-7000
Attorney for Applicant

Electronic Acknowledgement Receipt

EFS ID:	17799986
Application Number:	11768729
International Application Number:	
Confirmation Number:	3536
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Customer Number:	37462
Filer:	Marcus E. Browne
Filer Authorized By:	
Attorney Docket Number:	W0537-700620
Receipt Date:	02-JAN-2014
Filing Date:	26-JUN-2007
Time Stamp:	14:24:43
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		-_Response_to_Non-Final_Office_Action_mailed_10-2-13_FINAL.pdf	64020 8ede93ea4d0ed5c571606a2091201455577ced85	yes	16

Multipart Description/PDF files in .zip description			
Document Description		Start	End
Amendment/Req. Reconsideration-After Non-Final Reject		1	1
Claims		2	10
Applicant Arguments/Remarks Made in an Amendment		11	16

Warnings:

Information:

Total Files Size (in bytes):

64020

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 11/768,729	Filing Date 06/26/2007	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

ENTITY: LARGE SMALL MICRO

APPLICATION AS FILED – PART I

FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)
<input type="checkbox"/> BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>	N/A	N/A	N/A	
<input type="checkbox"/> SEARCH FEE <small>(37 CFR 1.16(k), (l), or (m))</small>	N/A	N/A	N/A	
<input type="checkbox"/> EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A	N/A	
TOTAL CLAIMS <small>(37 CFR 1.16(i))</small>	minus 20 =	*	X \$ =	
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>	minus 3 =	*	X \$ =	
<input type="checkbox"/> APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.16(j))</small>				
<small>* If the difference in column 1 is less than zero, enter "0" in column 2.</small>			TOTAL	

APPLICATION AS AMENDED – PART II

	(Column 1)	(Column 2)	(Column 3)	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)
AMENDMENT	01/02/2014	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR			
	Total <small>(37 CFR 1.16(i))</small>	* 38	Minus	** 38	= 0	X \$40 = 0
	Independent <small>(37 CFR 1.16(h))</small>	* 4	Minus	***4	= 0	X \$210 = 0
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>					
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>					
					TOTAL ADD'L FEE	0

	(Column 1)	(Column 2)	(Column 3)	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR			
	Total <small>(37 CFR 1.16(i))</small>	*	Minus	**	=	X \$ =
	Independent <small>(37 CFR 1.16(h))</small>	*	Minus	***	=	X \$ =
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>					
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>					
					TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
 ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
 *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
 The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
 /YOLANDA CHADWICK/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with 37 CFR § 1.6(a)(4).

Dated: January 31, 2014
Electronic Signature for Marcus E. Browne: / Marcus E. Browne /

Docket No.: W0537-700620
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Kenneth P. Weiss

Application No.: 11/768,729

Confirmation No.: 3536

Filed: June 26, 2007

Art Unit: 2435

For: UNIVERSAL SECURE REGISTRY

Examiner: Thomas A. Gyorfi

SUPPLEMENTAL AMENDMENT

Commissioner for Patents

Dear Madam:

INTRODUCTORY COMMENTS

In response to the Amendment filed on January 2, 2014 to the Office Action mailed October 2, 2013, and in response to the Examiner Interview conducted on January 24, 2014, please amend the above-identified U.S. patent application as follows:

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks begin on page 11 of this paper.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A secure registry system for providing information to a provider first party to enable transactions between the provider first party and entities with secure data stored in the secure registry system, the secure registry system comprising:

a database including secure data for each entity, wherein each entity is associated with a time-varying multicharacter code for each entity having secure data in the secure registry system, respectively, each time-varying multicharacter code representing an identity of one of the respective entities; and

a processor configured to receive a transaction request including at least the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed and an indication of the provider first party requesting the transaction, ~~configured~~ to map the time-varying multicharacter code to the identity of the entity ~~in the database~~ using the time-varying multicharacter code, to execute a restriction mechanism ~~configured~~ to determine compliance with any access restrictions for the provider first party to secure data of the entity for completing the transaction based at least in part on the indication of the first party and the time-varying multicharacter code of the transaction request, and to allow or not allow access to the secure data associated with the entity including information required to enable the transaction based on the determined compliance with any access restrictions for the provider first party, the information including account identifying information, wherein the account identifying information is not provided to the provider first party and the account identifying information is provided to a third party to enable or deny the transaction with the provider first party without providing the account identifying information to the provider first party.

2. (Canceled)

3. (Previously Presented) The system of claim 1, wherein the time-varying multicharacter code is provided to the system via a secure electronic transmission device.

4. (Previously Presented) The system of claim 1, wherein the time-varying multicharacter code is encrypted and transmitted to the system, and

wherein the system is configured to decrypt the time-varying multicharacter code with a public key of the entity.

5. (Currently Amended) The system as claimed in claim 1, wherein the transaction includes a service provided by the provider ~~first party~~,

wherein said provider's ~~first party's~~ service includes delivery,

wherein the information is an address to which an item is to be delivered to the entity,

wherein the system receives the time-varying multicharacter code, and

wherein the system uses the time-varying multicharacter code to obtain the appropriate address for delivery of the item by the third party.

6. – 8. (Canceled)

9. (Previously Presented) The system as claimed in claim 1, wherein the account identifying information includes credit card account information regarding the entity, and wherein the processor is configured to provide the credit card account information based upon the multicharacter code of the entity to enable the transaction.

10. (Previously Presented) The system as claimed in claim 9, wherein the system is configured to receive an approval of the credit card transaction.

11. (Previously Presented) The system as claimed in claim 1, wherein the account identifying information includes bank card account information regarding the entity, and wherein the processor

is configured to provide the bank card account information to enable the transaction based upon the multicharacter code of the entity.

12. (Previously Presented) The system as claimed in claim 11, wherein the system is configured to provide an approval of the bank card transaction.

13. (Previously Presented) The system as claimed in claim 1, wherein the information includes personal identification information regarding the entity.

14. (Currently Amended) The system as claimed in claim 13, wherein the personal identification information comprises a photograph of the entity, and wherein the photograph is provided to the provider first party.

15. (Previously Presented) The system as claimed in claim 1, wherein the account identifying information identifies email address information regarding the entity.

16. (Currently Amended) A method for providing information to a provider first party to enable transactions between the provider first party and entities who have secure data stored in a secure registry in which each entity is identified by a time-varying multicharacter code, the method comprising:

receiving a transaction request including at least the time-varying multicharacter code for an entity on whose behalf a transaction is to take place and an indication of the provider first party requesting the transaction;

mapping the time-varying multicharacter code to an identity of the entity ~~in a database~~ using the time-varying multicharacter code;

determining compliance with any access restrictions for the provider first party to secure data of the entity for completing the transaction based at least in part on the indication of the provider first party and the time-varying multicharacter code of the transaction request;

accessing information of the entity required to perform the transaction based on the determined compliance with any access restrictions for the provider first party, the information including account identifying information;

providing the account identifying information to a third party without providing the account identifying information to the provider first party to enable or deny the transaction; and

enabling or denying the provider first party to perform the transaction without the provider's first party's knowledge of the account identifying information.

17. – 18. (Canceled)

19. (Previously Presented) The method of claim 16, wherein the act of receiving the time-varying multicharacter code comprises receiving the time-varying multicharacter code transmitted via a secure electronic transmission device.

20. (Previously Presented) The method of claim 16, wherein the act of receiving the time-varying multicharacter code comprises receiving an encrypted multicharacter code, and wherein the method further comprises decrypting the encrypted multicharacter code.

21. (Currently Amended) The method as claimed in claim 16, wherein the transaction includes a service provided by the provider first party, wherein the service includes delivery, wherein the account identifying information is associated with an address to which an item is to be delivered for the entity, and wherein the third party receives the address for delivery of an item provided by the provider first party.

22. – 23. (Canceled)

24. (Previously Presented) The method as claimed in claim 16, wherein the account identifying information includes a credit card number, and wherein the act of using the account identifying information comprises using the credit card number to enable the transaction.
25. (Currently Amended) The method as claimed in claim 24, wherein the act of using the account identifying information comprises receiving a validation or denial of the transaction without providing the credit card number of the entity to the provider ~~first party~~.
26. (Previously Presented) The method as claimed in claim 16, wherein the act of using the account identifying information comprises using bank card information about the entity to enable a transaction.
27. (Currently Amended) The method as claimed in claim 26, wherein the act of using the information comprises receiving a validation or denial of the bank card transaction without providing a bank card number of the entity to the provider ~~first party~~.
28. (Currently Amended) The method as claimed in claim 16, wherein the act of mapping the time-varying multicharacter code to information required by the provider ~~first party~~ comprises mapping the time-varying multicharacter code to personal identification information about the entity.
29. (Currently Amended) The method as claimed in claim 28, wherein the personal identification information comprises a photograph of the entity, and
wherein the method further comprises an act of providing the photograph to the provider ~~first party~~.
30. (Previously Presented) The method as claimed in claim 16, wherein the account identifying information identifies email address information about the entity.

31. (Canceled)

32. (Currently Amended) The method as claimed in claim 24, further comprising an act of transmitting to the provider ~~first party~~ one of an approval or a denial of the credit card transaction.

33. (Previously Presented) The system of claim 1, wherein the database is further configured to associate biometric information with each entity having secure data in the secure registry, respectively.

34. (Currently Amended) The system of claim 33, wherein the processor is further configured to map the time-varying multicharacter code to biometric information associated with the entity on whose behalf the transaction is to be performed and to provide the biometric information to the provider ~~first party~~.

35. (Previously Presented) The system of claim 34, wherein the biometric information includes an image of the entity on whose behalf the transaction is to be performed.

36. (Previously Presented) The system of claim 34, wherein the time-varying multicharacter code is generated by a device associated with the entity on whose behalf the transaction is to be performed.

37. (Previously Presented) The method as claimed in claim 16, further comprising an act of associating biometric information with each entity having secure data in the secure registry, respectively.

38. (Currently Amended) The method of claim 37, further comprising acts of:
mapping the time-varying multicharacter code to biometric information associated with the entity on whose behalf the transaction is to be performed; and
providing the biometric information to the provider ~~first party~~.

39. (Previously Presented) The method of claim 38, wherein the biometric information includes an image of the entity on whose behalf the transaction is to be performed.
40. (Canceled)
41. (Previously Presented) The system of claim 1, wherein the account identifying information includes an account number.
42. (Previously Presented) The system of claim 41, wherein the account identifying information includes credit card account information and the account number includes a credit card number.
43. (Previously Presented) The system of claim 41, wherein the third party includes a financial service provider and the account number includes at least one of a debit card number and a credit card number.
44. (Currently Amended) The system of claim 43, wherein the provider first party includes a merchant, and the service includes a sale of at least one of goods and services.
45. (Currently Amended) The system of claim 44, wherein the processor is further configured to receive, from the provider first party, a merchant ID, and a purchase amount.
46. (Previously Presented) The system of claim 1, wherein the identity of the entity is unknown until the time-varying code is mapped to the identity by the processor.
47. (Currently Amended) A secure registry system for providing information to a provider first party to enable transactions between the provider first party and entities with secure data stored in the secure registry system, the secure registry system comprising:

a database including secure data for each entity, wherein each entity is associated with a time-varying multicharacter code for each entity having secure data in the secure registry system, respectively, each time-varying multicharacter code representing an identity of one of the respective entities, wherein the database is configured to permit or deny access to information on the respective entity using the time-varying multicharacter code; and

a processor configured to receive the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed, configured to map the time-varying multicharacter code to the identity of the entity to identify the entity, configured to execute a restriction mechanism to determine compliance with any access restrictions for the provider first party to at least one portion of secure data for completing the transaction and to store an appropriate code with each such portion of secure data, configured to obtain from the database the secure data associated with the entity including information required to enable the transaction, the information including account identifying information, and configured to provide the account identifying information to a third party to enable or deny the transaction without providing the account identifying information to the provider first party.

48. (Currently Amended) A secure registry system for providing information to a provider first party to enable transactions between the provider first party and entities with secure data stored in the secure registry system, the secure registry system comprising:

a database including secure data for each entity, wherein each entity is associated with a time-varying multicharacter code for each entity having secure data in the secure registry system, respectively, each time-varying multicharacter code representing an identity of one of the respective entities; and

a processor configured to receive the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed, configured to map the time-varying multicharacter code to the identity of the entity without requiring further information to identify the entity, configured to access from the database secure data associated with the entity including information required to enable the transaction, the information including account identifying information, and configured to provide the account identifying information to a third party to enable or deny the

transaction without providing the account identifying information to the provider first party, and wherein enabling or denying the transaction without providing account identifying information to the provider first party includes limiting transaction information provided by the secure registry system to the provider first party to transaction approval information.

REMARKS

Claims 1, 3-5, 9-16, 19-21, 24-30, 32-39, and 41-48 were previously pending in this application. Claims 1, 5, 14, 16, 21, 25, 27-29, 32, 34, 38, 44, 45, 47, and 48 have been amended. As a result claims 1, 3-5, 9-16, 19-21, 24-30, 32-39, and 41-48 are pending for examination with claims 1, 16, 47 and 48 being independent claims. No new matter has been added.

Examiner Interview

Applicant wishes to thank Examiner Gyorfí for the courtesies extended to Applicant's Representatives during the course of the Interview conducted on January 24, 2014. During the course of the Interview, the participants discussed the Application, Office Action, the rejections of record and the amendments submitted in the response filed on January 2, 2014. Examiner Gyorfí suggested that the term "first party" could be misconstrued as being the consumer rather than the provider and suggested amending the claim to clarify the distinction to overcome the present rejection. Accordingly, Applicant has amended claims 1, 5, 14, 16, 21, 25, 27-29, 32, 34, 38, 44, 45, 47, and 48 to recite "provider" rather than "first party" per the Examiner's suggestion.

CONCLUSION

In view of the foregoing amendments and remarks, reconsideration is respectfully requested. This application should now be in condition for allowance; a notice to this effect is respectfully requested. If the Examiner believes, after this amendment, that the application is not in condition for allowance, the Examiner is requested to call the Applicant's attorney at the telephone number listed below.

If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee that is not covered by an accompanying payment, please charge any deficiency to Deposit Account No. 50/2762 (Ref. No. W0537-700620).

Dated: January 31, 2014

Respectfully submitted,

Electronic signature: / Marcus E. Browne /
Marcus E. Browne
Registration No.: 71,897
Matthew H. Grady
Registration No.: 52,957
LANDO & ANASTASI LLP
Riverfront Office Park
One Main Street
Suite 1100
Cambridge, Massachusetts 02142
(617) 395-7000
Attorney for Applicant

Electronic Acknowledgement Receipt

EFS ID:	18085424
Application Number:	11768729
International Application Number:	
Confirmation Number:	3536
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Customer Number:	37462
Filer:	Marcus E. Browne
Filer Authorized By:	
Attorney Docket Number:	W0537-700620
Receipt Date:	31-JAN-2014
Filing Date:	26-JUN-2007
Time Stamp:	16:39:45
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no
------------------------	----

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		- _SUPPLEMENTAL_Response_to _Non- Final_Office_Action_mailed_10 -2-13_FINAL.pdf	48162 e95af4196286a722432c69347b4e5537cd7 5ac24	yes	12

Multipart Description/PDF files in .zip description			
Document Description		Start	End
Supplemental Response or Supplemental Amendment		1	1
Claims		2	10
Applicant Arguments/Remarks Made in an Amendment		11	12

Warnings:

Information:

Total Files Size (in bytes):	48162
-------------------------------------	-------

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD Substitute for Form PTO-875	Application or Docket Number 11/768,729	Filing Date 06/26/2007	<input type="checkbox"/> To be Mailed
---	---	----------------------------------	---------------------------------------

ENTITY: LARGE SMALL MICRO

APPLICATION AS FILED – PART I

FOR	NUMBER FILED	NUMBER EXTRA	RATE (\$)	FEE (\$)
<input type="checkbox"/> BASIC FEE <small>(37 CFR 1.16(a), (b), or (c))</small>	N/A	N/A	N/A	
<input type="checkbox"/> SEARCH FEE <small>(37 CFR 1.16(k), (l), or (m))</small>	N/A	N/A	N/A	
<input type="checkbox"/> EXAMINATION FEE <small>(37 CFR 1.16(o), (p), or (q))</small>	N/A	N/A	N/A	
TOTAL CLAIMS <small>(37 CFR 1.16(i))</small>	minus 20 =	*	X \$ =	
INDEPENDENT CLAIMS <small>(37 CFR 1.16(h))</small>	minus 3 =	*	X \$ =	
<input type="checkbox"/> APPLICATION SIZE FEE <small>(37 CFR 1.16(s))</small>	If the specification and drawings exceed 100 sheets of paper, the application size fee due is \$310 (\$155 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).			
<input type="checkbox"/> MULTIPLE DEPENDENT CLAIM PRESENT <small>(37 CFR 1.16(j))</small>				
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL	

APPLICATION AS AMENDED – PART II

	(Column 1)	(Column 2)	(Column 3)	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	
AMENDMENT	01/31/2014	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR				
	Total <small>(37 CFR 1.16(i))</small>	* 38	Minus	** 38	= 0	X \$40 = 0	
	Independent <small>(37 CFR 1.16(h))</small>	* 4	Minus	***4	= 0	X \$210 = 0	
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>						
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>						
					TOTAL ADD'L FEE	0	

	(Column 1)	(Column 2)	(Column 3)	PRESENT EXTRA	RATE (\$)	ADDITIONAL FEE (\$)	
AMENDMENT		CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR				
	Total <small>(37 CFR 1.16(i))</small>	*	Minus	**	=	X \$ =	
	Independent <small>(37 CFR 1.16(h))</small>	*	Minus	***	=	X \$ =	
	<input type="checkbox"/> Application Size Fee <small>(37 CFR 1.16(s))</small>						
	<input type="checkbox"/> FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <small>(37 CFR 1.16(j))</small>						
					TOTAL ADD'L FEE		

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
 ** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
 *** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
 The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

LIE
 /PHYLLIS CANTY/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/768,729	06/26/2007	Kenneth P. Weiss	W0537-700620	3536
37462	7590	02/04/2014	EXAMINER	
LANDO & ANASTASI, LLP ONE MAIN STREET, SUITE 1100 CAMBRIDGE, MA 02142			GYORFI, THOMAS A	
			ART UNIT	PAPER NUMBER
			2435	
			NOTIFICATION DATE	DELIVERY MODE
			02/04/2014	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@LALaw.com
gengelso@LALaw.com

Applicant-Initiated Interview Summary	Application No. 11/768,729	Applicant(s) WEISS, KENNETH P.	
	Examiner Thomas Gyorfi	Art Unit 2435	

All participants (applicant, applicant's representative, PTO personnel):

- (1) Thomas Gyorfi. (3) Matthew Grady (Applicant's representative).
(2) Marcus Browne (Applicant's representative). (4) John Anastasi (Applicant's representative).

Date of Interview: 24 January 2014.

Type: Telephonic Video Conference
 Personal [copy given to: applicant applicant's representative]

Exhibit shown or demonstration conducted: Yes No.
If Yes, brief description: _____.

Issues Discussed 101 112 102 103 Others
(For each of the checked box(es) above, please describe below the issue and detailed description of the discussion)

Claim(s) discussed: 1,16,47 and 48.

Identification of prior art discussed: Giordano (US 7571139), Keresman (US 7742967).

Substance of Interview

(For each issue discussed, provide a detailed description and indicate if agreement was reached. Some topics may include: identification or clarification of a reference or a portion thereof, claim interpretation, proposed amendments, arguments of any applied references etc...)

Examiner and Applicant's representatives discussed the instant invention, noting that in the preferred embodiment the "first party" is intended to represent a merchant - thus entailing that the invention provides an identifier of the merchant associated with a time-varying multicharacter code of the customer. While the Examiner conceded that that embodiment would overcome the prior art of record, Examiner maintained that the claims were broad enough to allow for an alternative interpretation wherein the "first party" is the customer, thus allowing the current rejections to stand. Examiner suggested a Supplemental Amendment to further clarify the nature of the first party to distinguish the claimed invention over the prior art of record..

Applicant recordation instructions: The formal written reply to the last Office action must include the substance of the interview. (See MPEP section 713.04). If a reply to the last Office action has already been filed, applicant is given a non-extendable period of the longer of one month or thirty days from this interview date, or the mailing date of this interview summary form, whichever is later, to file a statement of the substance of the interview

Examiner recordation instructions: Examiners must summarize the substance of any interview of record. A complete and proper recordation of the substance of an interview should include the items listed in MPEP 713.04 for complete and proper recordation including the identification of the general thrust of each argument or issue discussed, a general indication of any other pertinent matters discussed regarding patentability and the general results or outcome of the interview, to include an indication as to whether or not agreement was reached on the issues raised.

Attachment

/Darren B Schwartz/
Primary Examiner, Art Unit 2435

/Thomas Gyorfi/
Examiner, Art Unit 2435

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record

A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews

Paragraph (b)

In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.

All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:

- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:

- 1) A brief description of the nature of any exhibit shown or any demonstration conducted,
- 2) an identification of the claims discussed,
- 3) an identification of the specific prior art discussed,
- 4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
- 5) a brief identification of the general thrust of the principal arguments presented to the examiner,
(The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
- 6) a general indication of any other pertinent matters discussed, and
- 7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.



NOTICE OF ALLOWANCE AND FEE(S) DUE

37462 7590 02/28/2014
LANDO & ANASTASI, LLP
ONE MAIN STREET, SUITE 1100
CAMBRIDGE, MA 02142

EXAMINER
GYORFI, THOMAS A
ART UNIT PAPER NUMBER

2435

DATE MAILED: 02/28/2014

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.

TITLE OF INVENTION: UNIVERSAL SECURE REGISTRY

Table with 7 columns: APPLN. TYPE, ENTITY STATUS, ISSUE FEE DUE, PUBLICATION FEE DUE, PREV. PAID ISSUE FEE, TOTAL FEE(S) DUE, DATE DUE

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

**Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE
 Commissioner for Patents
 P.O. Box 1450
 Alexandria, Virginia 22313-1450
 or Fax (571)-273-2885**

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

37462 7590 02/28/2014
LANDO & ANASTASI, LLP
 ONE MAIN STREET, SUITE 1100
 CAMBRIDGE, MA 02142

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/768,729	06/26/2007	Kenneth P. Weiss	W0537-700620	3536

TITLE OF INVENTION: UNIVERSAL SECURE REGISTRY

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$480	\$0	\$0	\$480	05/28/2014

EXAMINER	ART UNIT	CLASS-SUBCLASS
GYORFI, THOMAS A	2435	713-182000

<p>1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).</p> <p><input type="checkbox"/> Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.</p> <p><input type="checkbox"/> "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. Use of a Customer Number is required.</p>	<p>2. For printing on the patent front page, list</p> <p>(1) The names of up to 3 registered patent attorneys or agents OR, alternatively, _____ 1</p> <p>(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. _____ 2</p> <p>_____ 3</p>
---	---

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE _____ (B) RESIDENCE: (CITY and STATE OR COUNTRY) _____

Please check the appropriate assignee category or categories (will not be printed on the patent) : Individual Corporation or other private group entity Government

<p>4a. The following fee(s) are submitted:</p> <p><input type="checkbox"/> Issue Fee</p> <p><input type="checkbox"/> Publication Fee (No small entity discount permitted)</p> <p><input type="checkbox"/> Advance Order - # of Copies _____</p>	<p>4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)</p> <p><input type="checkbox"/> A check is enclosed.</p> <p><input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.</p> <p><input type="checkbox"/> The Director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).</p>
---	---

5. **Change in Entity Status** (from status indicated above)

Applicant certifying micro entity status. See 37 CFR 1.29

Applicant asserting small entity status. See 37 CFR 1.27

Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
Values: 11/768,729, 06/26/2007, Kenneth P. Weiss, W0537-700620, 3536

37462 7590 02/28/2014
LANDO & ANASTASI, LLP
ONE MAIN STREET, SUITE 1100
CAMBRIDGE, MA 02142

EXAMINER

GYORFI, THOMAS A

ART UNIT PAPER NUMBER

2435

DATE MAILED: 02/28/2014

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 105 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 105 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 11/768,729	Applicant(s) WEISS, KENNETH P.	
	Examiner Thomas Gyorfi	Art Unit 2435	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. This communication is responsive to See Continuation Sheet.
 A declaration(s)/affidavit(s) under **37 CFR 1.130(b)** was/were filed on _____.
2. An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. The allowed claim(s) is/are 1,3-5,9-16,19-21,24-30,32-39 and 41-48. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.
4. Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

- a) All b) Some *c) None of the:
1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has **THREE MONTHS FROM THE "MAILING DATE"** of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in **ABANDONMENT** of this application.

THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. **CORRECTED DRAWINGS** (as "replacement sheets") must be submitted.
 including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. **DEPOSIT OF and/or INFORMATION** about the deposit of **BIOLOGICAL MATERIAL** must be submitted. Note the attached Examiner's comment regarding **REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL**.

Attachment(s)

- | | |
|--|--|
| 1. <input type="checkbox"/> Notice of References Cited (PTO-892) | 5. <input type="checkbox"/> Examiner's Amendment/Comment |
| 2. <input type="checkbox"/> Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date _____ | 6. <input checked="" type="checkbox"/> Examiner's Statement of Reasons for Allowance |
| 3. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit
of Biological Material | 7. <input type="checkbox"/> Other _____. |
| 4. <input type="checkbox"/> Interview Summary (PTO-413),
Paper No./Mail Date _____. | |

/Thomas Gyorfi/
Examiner, Art Unit 2435

Continuation of Item 1. This communication is responsive to : the amendment filed 1/2/14 and the supplemental amendment filed 1/31/14.

DETAILED ACTION

1. Claims 1, 3-5, 9-16, 19-21, 24-30, 32-39, and 41-48 remain for examination. The amendment filed 1/2/14 amended claims 1, 16, 47 & 48; and the supplemental amendment filed 1/31/14 further amended claims 1, 5, 14, 16, 21, 25, 27-29, 32, 34, 38, 44, 45, 47, & 48.
2. The present application is being examined under the pre-AIA first to invent provisions.

Response to Arguments

3. Applicant's arguments, see the supplemental amendment filed 1/31/14, with respect to the rejections of the claims under 35 USC 103 have been fully considered and are persuasive. The rejection of claims 1-48 has been withdrawn.
4. Applicant's arguments from the amendment of 1/2/14 have been considered but are moot in view of the consideration of the supplemental amendment *supra*.

Allowable Subject Matter

5. Claims 1, 3-5, 9-16, 19-21, 24-30, 32-39, and 41-48 are allowed.
6. The following is an examiner's statement of reasons for allowance: the claims were amended to stipulate that a provider of goods & services [e.g. a merchant] performs the step of providing the time-varying multicharacter code of an entity [e.g. customer] to a third party to determine if a transaction should be allowed to proceed; in contrast, the prior art teaches the customer providing his time-varying multicharacter code to a third party to authenticate access to the merchant's web site (see also the

Art Unit: 2435

Interview Summary mailed 2/4/14). The Examiner could find no other prior art that would teach or suggest the amended limitations.

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas Gyorfi whose telephone number is (571)272-3849. The examiner can normally be reached on 10:00am - 6:30pm Monday - Friday.


If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Joseph Hirl can be reached on (571) 272-3685. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Art Unit: 2435

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Thomas Gyorfi/
Examiner, Art Unit 2435
2/14/14

/Darren B Schwartz/
Primary Examiner, Art Unit 2435

Index of Claims 	Application/Control No. 11768729	Applicant(s)/Patent Under Reexamination WEISS, KENNETH P.
	Examiner BEEMNET W DADA	Art Unit 2435

✓	Rejected
=	Allowed


-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

Claims renumbered in the same order as presented by applicant
 CPA
 T.D.
 R.1.47

CLAIM		DATE							
Final	Original	07/16/2009	09/25/2013	02/14/2014					
1	1	✓	✓	=					
	2	✓	-	-					
2	3	✓	✓	=					
3	4	✓	✓	=					
4	5	✓	✓	=					
	6	✓	-	-					
	7	✓	-	-					
	8	✓	-	-					
5	9	✓	✓	=					
6	10	✓	✓	=					
7	11	✓	✓	=					
8	12	✓	✓	=					
9	13	✓	✓	=					
10	14	✓	✓	=					
11	15	✓	✓	=					
22	16	✓	✓	=					
	17	✓	-	-					
	18	✓	-	-					
23	19	✓	✓	=					
24	20	✓	✓	=					
25	21	✓	✓	=					
	22	✓	-	-					
	23	✓	-	-					
26	24	✓	✓	=					
27	25	✓	✓	=					
29	26	✓	✓	=					
30	27	✓	✓	=					
31	28	✓	✓	=					
32	29	✓	✓	=					
33	30	✓	✓	=					
	31		-	-					
28	32		✓	=					
12	33		✓	=					
13	34		✓	=					
14	35		✓	=					
15	36		✓	=					

<i>Index of Claims</i> 	Application/Control No. 11768729	Applicant(s)/Patent Under Reexamination WEISS, KENNETH P.
	Examiner BEEMNET W DADA	Art Unit 2435

✓	Rejected
=	Allowed


-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected


Claims renumbered in the same order as presented by applicant
 CPA
 T.D.
 R.1.47

CLAIM		DATE							
Final	Original	07/16/2009	09/25/2013	02/14/2014					
34	37		✓	=					
35	38		✓	=					
36	39		✓	=					
	40		-	-					
16	41		✓	=					
17	42		✓	=					
18	43		✓	=					
19	44		✓	=					
20	45		✓	=					
21	46		✓	=					
37	47		✓	=					
38	48		✓	=					

Issue Classification 	Application/Control No. 11768729	Applicant(s)/Patent Under Reexamination WEISS, KENNETH P.
	Examiner THOMAS GYORFI	Art Unit 2435

<input type="checkbox"/> Claims renumbered in the same order as presented by applicant																<input type="checkbox"/> CPA		<input type="checkbox"/> T.D.		<input type="checkbox"/> R.1.47	
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original						
1	1		17	12	33																
	2		18	13	34																
2	3	23	19	14	35																
3	4	24	20	15	36																
4	5	25	21	34	37																
	6		22	35	38																
	7		23	36	39																
	8	26	24		40																
5	9	27	25	16	41																
6	10	29	26	17	42																
7	11	30	27	18	43																
8	12	31	28	19	44																
9	13	32	29	20	45																
10	14	33	30	21	46																
11	15		31	37	47																
22	16	28	32	38	48																

/THOMAS GYORFI/ Examiner.Art Unit 2435 (Assistant Examiner)	2/14/14 (Date)	Total Claims Allowed: 38	
/DARREN B SCHWARTZ/ Primary Examiner.Art Unit 2435 (Primary Examiner)	02/21/2014 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 1

Search Notes 	Application/Control No. 11768729	Applicant(s)/Patent Under Reexamination WEISS, KENNETH P.
	Examiner BEEMNET W DADA	Art Unit 2435

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
713	169, 182, 184	12/10/2012	BD
707	9	12/10/2012	BD
713	169, 182, 184	9/25/13	TAG
707	9	9/25/13	TAG
713	169, 182, 184	2/14/14	TAG
707	999.001	2/14/14	TAG

SEARCH NOTES		
Search Notes	Date	Examiner
East search	12/10/2012	BD
NPL search	12/10/2012	BD
Inventor name search	12/10/2012	BD
EAST search (updated)	9/25/13	TAG
Discussed allowability with SPE J. Hirl (AU2435)	2/10/14	TAG
EAST search (updated)	2/14/14	TAG
NPL search (Google)	2/14/14	TAG
Reviewed by Primary Examiner D. Schwartz (AU 2435)	2/14/14	TAG

INTERFERENCE SEARCH			
US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner

--	--

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
713	182	2/14/14	TAG

--	--

EAST Search History**EAST Search History (Prior Art)**

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	8315	weiss.in.	US-PGPUB; USPAT	OR	OFF	2014/02/21 19:00
L2	103	l1 and (ken.in. kenneth.in.)	US-PGPUB; USPAT	OR	OFF	2014/02/21 19:01
L3	7	(universal adj secure adj registry).as.	US-PGPUB; USPAT	OR	OFF	2014/02/21 19:01
L4	30	l2 and @ad<"20010316"	US-PGPUB; USPAT	OR	OFF	2014/02/21 19:02

EAST Search History (Interference)

<This search history is empty>

2/ 21/ 2014 7:02:15 PM

C:\ Users\ tgyorfi\ Documents\ EAST\ Workspaces\ 11768729.wsp

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1468	713/169.ccls.	US-PGPUB; USPAT	OR	OFF	2014/02/14 16:36
L2	3218	713/182.ccls.	US-PGPUB; USPAT	OR	OFF	2014/02/14 16:36
L3	979	713/184.ccls.	US-PGPUB; USPAT	OR	OFF	2014/02/14 16:36
L5	2933	707/999.009.ccls.	US-PGPUB; USPAT	OR	OFF	2014/02/14 16:36
L6	400	secure near2 registry	US-PGPUB; USPAT	OR	OFF	2014/02/14 16:48
L7	1	l6 and (provider same (token timecode (time near2 code)))	US-PGPUB; USPAT	OR	OFF	2014/02/14 16:48
L8	0	l6 and (provider same securid)	US-PGPUB; USPAT	OR	OFF	2014/02/14 16:49
L9	13	(l1 l2 l3 l5) and secure near2 registry	US-PGPUB; USPAT	OR	OFF	2014/02/14 16:49
L10	1	("20080005576").PN.	US-PGPUB; USPAT	OR	OFF	2014/02/14 17:29
S1	3	((("6018724") or ("7571139") or ("5657388")).PN.	US-PGPUB; USPAT	OR	OFF	2013/08/22 17:35
S2	8	US-6498861-\$.DID. OR US-7237117-\$.DID. OR US-5457747-\$.DID. OR US-6950521-\$.DID. OR US-8001055-\$.DID. OR US-7809651-\$.DID. OR US-7805372-\$.DID. OR US-8234220-\$.DID.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/08/23 15:40
S3	9	US-7766223-\$.DID. OR US-20030229637-\$.DID. OR US-20030046540-\$.DID. OR US-20020184538-\$.DID. OR US-20030028481-\$.DID. OR US-20030084332-\$.DID. OR US-20030085808-\$.DID. OR US-20050113070-\$.DID. OR US-20050238147-\$.DID.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/08/23 15:41
S4	6	US-20070256120-\$.DID. OR US-20090292641-\$.DID. OR US-20100000455-\$.DID. OR US-20110258120-\$.DID. OR US-20130024374-\$.DID. OR US-20120037479-\$.DID.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/08/23 15:42
S5	254	"5657388".uref.	US-PGPUB;	OR	OFF	2013/09/25 16:30

			USPAT			
S6	27	S5 and @ad<"20010316"	US-PGPUB; USPAT	OR	OFF	2013/09/25 16:31
S7	11	S6 and restrict\$3	US-PGPUB; USPAT	OR	OFF	2013/09/25 16:37
S8	1390	713/169.ccls.	US-PGPUB; USPAT	OR	OFF	2013/09/25 16:56
S9	3037	713/182.ccls.	US-PGPUB; USPAT	OR	OFF	2013/09/25 16:57
S10	917	713/184.ccls.	US-PGPUB; USPAT	OR	OFF	2013/09/25 16:57
S11	0	707/9.ccls.	US-PGPUB; USPAT	OR	OFF	2013/09/25 16:57
S12	2927	707/999.009.ccls.	US-PGPUB; USPAT	OR	OFF	2013/09/25 16:58
S13	1634	(S8 S9 S10 S12) and @ad<"20010316"	US-PGPUB; USPAT	OR	OFF	2013/09/25 16:58
S14	318	S13 and (token timecode (time near2 code))	US-PGPUB; USPAT	OR	OFF	2013/09/25 16:59
S15	152	S14 and restrict\$3	US-PGPUB; USPAT	OR	OFF	2013/09/25 16:59
S16	1	("7571139").PN.	US-PGPUB; USPAT	OR	OFF	2014/01/24 10:15

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L11	231	secure near2 registry	US-PGPUB; UPAD	OR	OFF	2014/02/14 17:33
L12	91107	(token timecode (time near2 code) securid)	US-PGPUB; UPAD	OR	OFF	2014/02/14 17:34
L13	104	l12 and l11	US-PGPUB; UPAD	OR	OFF	2014/02/14 17:34
L14	4980	l12 same provider	US-PGPUB; UPAD	OR	OFF	2014/02/14 17:34
L15	1	l14 and l11	US-PGPUB; UPAD	OR	OFF	2014/02/14 17:34

2/ 14/ 2014 5:35:17 PM

C:\Users\tygorfi\Documents\EAST\Workspaces\11768729.wsp

RSA SecurID Token Replacement and Disposal - EMC
www.emc.com/support/rsa/.../token-replacement.htm - EMC Corporation
 Feb 1, 2001 - Learn how to replace or dispose of RSA SecurID hardware authenticators. Tokens are replaced without charge if there are problems in materials or ...

Installing and Configuring SecurID - Portmasters.com
portmasters.com/www.livingston.com/tech/docs/.../securidconfig.html
 Feb 1, 2001 - Security Dynamics Technologies, Inc. provides an additional level of security in user identification and authentication by using SecurID tokens to generate codes ...

PDF: RSA SecurID Token Replacement - Cygate Group
www.cygategroup.com/upload/pdf/Support/Token_Replacements.pdf
 Feb 1, 2001 - Warranty. RSA Security warrants all RSA SecurID tokens for the purchased lifecycle. Tokens will be replaced without charge if they no longer operate properly ...

SMS HEALTHConX - More FAQs about tokens
<https://www.smshealthconx.net/HCtokenfaqs.htm>
 Feb 1, 2001 - ? A SecurID is a "smart" token. It contains a full CPU: a microprocessor, memory, and an output display. Machine ...

SecurID Tokens - Software Tokens (SD820...) - eSecurityToGo
www.esecuritytogo.com - RSA SecurID - RSA SecurID Tokens
 Feb 1, 2001 - RSA SecurID Software token functions like an RSA SecurID PINPAD card and provides the added benefit of allowing automated secure remote access.

PDF: Initial Cryptanalysis of the RSA SecurID Algorithm - Linux Security
www.linuxsecurity.com/resource_files/.../initial_securid_analysis.pdf
 Jan 31, 2001 - ularities in functions used within the SecurID algorithm: the time computation and final ... The RSA SecurID token is currently based upon a proprietary algorithm.

SecurID Installation
www.stat.ufl.edu/system/man/.../6securid.html - University of Florida
 Jan 28, 1998 - ACE/Server client: Machine generating the SecurID authentication attempt. Token: A small, handheld device that generates a random number. A new number is ...

Next: SecurID User Authentication Processing Details - Oracle ...
docs.oracle.com - Chapter 9 Authentication - Oracle Corporation
 Feb 1, 2001 - SecurID is a leading form of hardware-based authentication. SecurID authentication involves three components: a user-held hardware device (token), client ...

RFC 2808 - The SecurID(r) SASL Mechanism
<https://tools.ietf.org/html/rfc2808> - Internet Engineering Task...
 by M Nystrom - 2000 - Cited by 11 - Related articles
 Apr 15, 2000 - This memo assumes the reader has basic familiarity with the SecurID token, its associated authentication protocol and SASL. How to read this document The key ...

Bugtraq: Sample SecurID Token Emulator with Token Secret Import
seclists.org/bugtraq/2000/Dec/459
 Dec 21, 2000 - Sample SecurID Token Emulator with Token Secret Import We have performed some cryptanalysis and let's just say we do have grounds to believe that this ...

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

REQUEST FOR CONTINUED EXAMINATION(RCE)TRANSMITTAL (Submitted Only via EFS-Web)

Application Number	11768729	Filing Date	2007-06-26	Docket Number (if applicable)	W0537-700620	Art Unit	2435
First Named Inventor	Kenneth P. Weiss			Examiner Name	B. W. Dada		

This is a Request for Continued Examination (RCE) under 37 CFR 1.114 of the above-identified application.
Request for Continued Examination (RCE) practice under 37 CFR 1.114 does not apply to any utility or plant application filed prior to June 8, 1995, or to any design application. The Instruction Sheet for this form is located at WWW.USPTO.GOV

SUBMISSION REQUIRED UNDER 37 CFR 1.114

Note: If the RCE is proper, any previously filed unentered amendments and amendments enclosed with the RCE will be entered in the order in which they were filed unless applicant instructs otherwise. If applicant does not wish to have any previously filed unentered amendment(s) entered, applicant must request non-entry of such amendment(s).

Previously submitted. If a final Office action is outstanding, any amendments filed after the final Office action may be considered as a submission even if this box is not checked.

Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____

Other _____

Enclosed

Amendment/Reply

Information Disclosure Statement (IDS)

Affidavit(s)/ Declaration(s)

Other _____

MISCELLANEOUS

Suspension of action on the above-identified application is requested under 37 CFR 1.103(c) for a period of months _____
(Period of suspension shall not exceed 3 months; Fee under 37 CFR 1.17(i) required)

Other _____

FEES

The RCE fee under 37 CFR 1.17(e) is required by 37 CFR 1.114 when the RCE is filed.

The Director is hereby authorized to charge any underpayment of fees, or credit any overpayments, to Deposit Account No 50/2762

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Patent Practitioner Signature

Applicant Signature

Signature of Registered U.S. Patent Practitioner			
Signature	/Matthew H. Grady/	Date (YYYY-MM-DD)	2014-03-28
Name	Matthew H. Grady	Registration Number	52957

This collection of information is required by 37 CFR 1.114. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

PCT

NOTIFICATION OF TRANSMITTAL OF
THE INTERNATIONAL SEARCH REPORT AND
THE WRITTEN OPINION OF THE INTERNATIONAL
SEARCHING AUTHORITY, OR THE DECLARATION

To:

LOWRIE, LANDO & ANASTASI, LLP
Attn. Anastasi, John N.
One Main Street Suite 1100
Cambridge, MA 02142
ETATS-UNIS D'AMERIQUE

(PCT Rule 44.1)

Date of mailing (day/month/year) 11/03/2008	
Applicant's or agent's file reference W0537-7010W0	FOR FURTHER ACTION See paragraphs 1 and 4 below
International application No. PCT/US2007/070701	International filing date (day/month/year) 08/06/2007
Applicant WEISS, Kenneth P.	COPY

1. The applicant is hereby notified that the international search report and the written opinion of the International Searching Authority have been established and are transmitted herewith.

Filing of amendments and statement under Article 19:

The applicant is entitled, if he so wishes, to amend the claims of the International Application (see Rule 46):

When? The time limit for filing such amendments is normally two months from the date of transmittal of the International Search Report.

Where? Directly to the International Bureau of WIPO, 34 chemin des Colombettes
1211 Geneva 20, Switzerland, Facsimile No.: (41-22) 338.82.70

For more detailed instructions, see the notes on the accompanying sheet.

2. The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(a) to that effect and the written opinion of the International Searching Authority are transmitted herewith.

3. **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

- the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.
 no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. Reminders


Shortly after the expiration of **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in Rules 90*bis*.1 and 90*bis*.3, respectively, before the completion of the technical preparations for international publication.

The applicant may submit comments on an informal basis on the written opinion of the International Searching Authority to the International Bureau. The International Bureau will send a copy of such comments to all designated Offices unless an international preliminary examination report has been or is to be established. These comments would also be made available to the public but not before the expiration of 30 months from the priority date.

Within **19 months** from the priority date, but only in respect of some designated Offices, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase **until 30 months** from the priority date (in some Offices even later); otherwise, the applicant must, **within 20 months** from the priority date, perform the prescribed acts for entry into the national phase before those designated Offices.

In respect of other designated Offices, the time limit of **30 months** (or later) will apply even if no demand is filed within 19 months.

See the Annex to Form PCT/IB/301 and, for details about the applicable time limits, Office by Office, see the *PCT Applicant's Guide*, Volume II, National Chapters and the WIPO Internet site.

Name and mailing address of the International Searching Authority  European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Pilvi Koski
--	--

NOTES TO FORM PCT/ISA/220

These Notes are intended to give the basic instructions concerning the filing of amendments under article 19. The Notes are based on the requirements of the Patent Cooperation Treaty, the Regulations and the Administrative Instructions under that Treaty. In case of discrepancy between these Notes and those requirements, the latter are applicable. For more detailed information, see also the *PCT Applicant's Guide*, a publication of WIPO.

In these Notes, "Article", "Rule", and "Section" refer to the provisions of the PCT, the PCT Regulations and the PCT Administrative Instructions, respectively.

INSTRUCTIONS CONCERNING AMENDMENTS UNDER ARTICLE 19

The applicant has, after having received the international search report and the written opinion of the International Searching Authority, one opportunity to amend the claims of the international application. It should however be emphasized that, since all parts of the international application (claims, description and drawings) may be amended during the international preliminary examination procedure, there is usually no need to file amendments of the claims under Article 19 except where, e.g. the applicant wants the latter to be published for the purposes of provisional protection or has another reason for amending the claims before international publication. Furthermore, it should be emphasized that provisional protection is available in some States only (see *PCT Applicant's Guide*, Volume I/A, Annexes B1 and B2).

The attention of the applicant is drawn to the fact that amendments to the claims under Article 19 are not allowed where the International Searching Authority has declared, under Article 17(2), that no international search report would be established (see *PCT Applicant's Guide*, Volume I/A, paragraph 296).

What parts of the international application may be amended?

Under Article 19, only the claims may be amended.

During the international phase, the claims may also be amended (or further amended) under Article 34 before the International Preliminary Examining Authority. The description and drawings may only be amended under Article 34 before the International Examining Authority.

Upon entry into the national phase, all parts of the international application may be amended under Article 28 or, where applicable, Article 41.

When?

Within 2 months from the date of transmittal of the international search report or 16 months from the priority date, whichever time limit expires later. It should be noted, however, that the amendments will be considered as having been received on time if they are received by the International Bureau after the expiration of the applicable time limit but before the completion of the technical preparations for international publication (Rule 46.1).

Where not to file the amendments?

The amendments may only be filed with the International Bureau and not with the receiving Office or the International Searching Authority (Rule 46.2).

Where a demand for international preliminary examination has been/is filed, see below.

How?

Either by cancelling one or more entire claims, by adding one or more new claims or by amending the text of one or more of the claims as filed.

A replacement sheet must be submitted for each sheet of the claims which, on account of an amendment or amendments, differs from the sheet originally filed.

All the claims appearing on a replacement sheet must be numbered in Arabic numerals. Where a claim is cancelled, no renumbering of the other claims is required. In all cases where claims are renumbered, they must be renumbered consecutively (Section 205(b)).

The amendments must be made in the language in which the international application is to be published.

What documents must/may accompany the amendments?

Letter (Section 205(b)):

The amendments must be submitted with a letter.

The letter will not be published with the international application and the amended claims. It should not be confused with the "Statement under Article 19(1)" (see below, under "Statement under Article 19(1)").

The letter must be in English or French, at the choice of the applicant. However, if the language of the international application is English, the letter must be in English; if the language of the international application is French, the letter must be in French.

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference W0537-7010WO	FOR FURTHER ACTION		see Form PCT/ISA/220 as well as, where applicable, item 5 below.
International application No. PCT/US2007/070701	International filing date (day/month/year) 08/06/2007	(Earliest) Priority Date (day/month/year) 09/06/2006	
Applicant WEISS, Kenneth P.			

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 4 sheets.

It is also accompanied by a copy of each prior art document cited in this report.

1. Basis of the report

a. With regard to the **language**, the international search was carried out on the basis of:

- the International application in the language in which it was filed
- a translation of the international application into _____, which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1(b))

b. This international search report has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43.6bis(a)).

c. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, see Box No. I.

2. **Certain claims were found unsearchable** (See Box No. II)

3. **Unity of invention is lacking** (see Box No III)

4. With regard to the **title**,

- the text is approved as submitted by the applicant
- the text has been established by this Authority to read as follows:

5. With regard to the **abstract**,

- the text is approved as submitted by the applicant
- the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box No. IV. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority

6. With regard to the **drawings**,

a. the figure of the **drawings** to be published with the abstract is Figure No. 21

- as suggested by the applicant
- as selected by this Authority, because the applicant failed to suggest a figure
- as selected by this Authority, because this figure better characterizes the invention

b. none of the figures is to be published with the abstract

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06F21/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06F G07C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 2004/034771 A1 (EDGETT JEFF STEVEN [US] ET AL) 19 February 2004 (2004-02-19) figure 3 paragraph [0048] - paragraph [0050]	1,27-32, 38-40
X	US 2001/044900 A1 (UCHIDA KAORU [JP]) 22 November 2001 (2001-11-22) paragraph [0039]; figure 4	2-10,41, 42,67-75
X	US 2005/039027 A1 (SHAPIRO MICHAEL F [US]) 17 February 2005 (2005-02-17) abstract figure 2 paragraph [0015] - paragraph [0017] paragraph [0021] - paragraph [0022] paragraph [0024]	41-44

 Further documents are listed in the continuation of Box C. See patent family annex.

* Special categories of cited documents :

- *A* document defining the general state of the art which is not considered to be of particular relevance
- *E* earlier document but published on or after the international filing date
- *L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- *O* document referring to an oral disclosure, use, exhibition or other means
- *P* document published prior to the international filing date but later than the priority date claimed

- *T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- *X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- *Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- *Z* document member of the same patent family

Date of the actual completion of the international search

26 February 2008

Date of mailing of the international search report

11/03/2008

Name and mailing address of the ISA/

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Chabot, Pedro

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT.

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 986 209 A (MITSUBISHI ELECTRIC CORP [JP]) 15 March 2000 (2000-03-15) paragraph [0012] - paragraph [0013] -----	1-75

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2007/070701

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 2004034771	A1	19-02-2004	NONE
US 2001044900	A1	22-11-2001	JP 2001325549 A
US 2005039027	A1	17-02-2005	NONE
EP 0986209	A	15-03-2000	AU 718480 B2
			AU 3912199 A
			CN 1248114 A
			DE 69929267 T2
			HK 1026542 A1
			JP 2000092046 A
			US 6751733 B1

PATENT COOPERATION TREATY

From the
INTERNATIONAL SEARCHING AUTHORITY

PCT

To:

see form PCT/ISA/220

WRITTEN OPINION OF THE
INTERNATIONAL SEARCHING AUTHORITY
(PCT Rule 43bis.1)

Date of mailing
(day/month/year) see form PCT/ISA/210 (second sheet)

Applicant's or agent's file reference see form PCT/ISA/220	FOR FURTHER ACTION See paragraph 2 below
---	--

International application No. PCTUS2007/070701	International filing date (day/month/year) 08.06.2007	Priority date (day/month/year) 09.06.2006
---	--	--

International Patent Classification (IPC) or both national classification and IPC
INV. G06F21/00

Applicant
WEISS, Kenneth P.

1. This opinion contains indications relating to the following items:

- Box No. I Basis of the opinion
- Box No. II Priority
- Box No. III Non-establishment of opinion with regard to novelty, inventive step and industrial applicability
- Box No. IV Lack of unity of invention
- Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
- Box No. VI Certain documents cited
- Box No. VII Certain defects in the international application
- Box No. VIII Certain observations on the international application


2. **FURTHER ACTION**

If a demand for international preliminary examination is made, this opinion will usually be considered to be a written opinion of the International Preliminary Examining Authority ("IPEA") except that this does not apply where the applicant chooses an Authority other than this one to be the IPEA and the chosen IPEA has notified the International Bureau under Rule 66.1bis(b) that written opinions of this International Searching Authority will not be so considered.

If this opinion is, as provided above, considered to be a written opinion of the IPEA, the applicant is invited to submit to the IPEA a written reply together, where appropriate, with amendments, before the expiration of 3 months from the date of mailing of Form PCT/ISA/220 or before the expiration of 22 months from the priority date, whichever expires later.

For further options, see Form PCT/ISA/220.

3. For further details, see notes to Form PCT/ISA/220.

<p>Name and mailing address of the ISA:</p>  <p>European Patent Office D-80298 Munich Tel. +49 89 2399 - 0 Tx: 523656 epmu d Fax: +49 89 2399 - 4465</p>	<p>Date of completion of this opinion</p> <p>see form PCT/ISA/210</p>	<p>Authorized Officer</p> <p>Chabot, Pedro</p> <p>Telephone No. +49 89 2399-6085</p>
--	---	--



Box No. I Basis of the opinion

1. With regard to the **language**, this opinion has been established on the basis of:
 - the international application in the language in which it was filed
 - a translation of the international application into , which is the language of a translation furnished for the purposes of international search (Rules 12.3(a) and 23.1 (b)).
2. This opinion has been established taking into account the **rectification of an obvious mistake** authorized by or notified to this Authority under Rule 91 (Rule 43bis.1(a))
3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application and necessary to the claimed invention, this opinion has been established on the basis of:
 - a. type of material:
 - a sequence listing
 - table(s) related to the sequence listing
 - b. format of material:
 - on paper
 - in electronic form
 - c. time of filing/furnishing:
 - contained in the international application as filed.
 - filed together with the international application in electronic form.
 - furnished subsequently to this Authority for the purposes of search.
4. In addition, in the case that more than one version or copy of a sequence listing and/or table relating thereto has been filed or furnished, the required statements that the information in the subsequent or additional copies is identical to that in the application as filed or does not go beyond the application as filed, as appropriate, were furnished.
5. Additional comments:

Box No. V Reasoned statement under Rule 43bis.1(a)(i) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. Statement

Novelty (N)	Yes: Claims	<u>11-26,33-37,45-66</u>
	No: Claims	<u>1-10,27-32,38-44,67-75</u>
Inventive step (IS)	Yes: Claims	
	No: Claims	<u>1-75</u>
Industrial applicability (IA)	Yes: Claims	<u>1-75</u>
	No: Claims	

2. Citations and explanations

see separate sheet

Re Item V.

1 Reference is made to the following documents:

- D1 : US 2004/034771 A1 (EDGETT JEFF STEVEN [US] ET AL) 19 February 2004 (2004-02-19)
- D2 : EP 0 986 209 A (MITSUBISHI ELECTRIC CORP [JP]) 15 March 2000 (2000-03-15)
- D3 : US 2001/044900 A1 (UCHIDA KAORU [JP]) 22 November 2001 (2001-11-22)
- D4 : US 2005/039027 A1 (SHAPIRO MICHAEL F [US]) 17 February 2005 (2005-02-17)

2 The present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of claim 1 is not new in the sense of Article 33(2) PCT.

Document D1 discloses (the references in parentheses applying to this document):

- a) A method of authenticating an identity of a first entity (Par. 48-50).
- b) Wirelessly transmitting from a first device, first encrypted authentication information of the first entity (par. 49 lines 3-8, It is considered that the network includes wireless means that are being used in the transmission).
- c) Receiving with a second device the wirelessly transmitted first encrypted authentication information (par. 49 line 8).
- d) Decrypting with the second device, the first wirelessly encrypted authentication information to provide the first authentication information of the first entity to the second device (par. 49 lines 20-24).
- e) Authenticating the identity of the first entity based upon the first authentication information and acting based on the authenticated identity of the first entity (par. 50).

3 The present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of claim 41 is not new in the sense of Article 33(2) PCT.

Document D4 discloses (the references in parentheses applying to this document):

- a) A system for validating an identity of a first entity comprising a first wireless device comprising (par. 5).
 - b) A first wireless transmitter and receiver configured to transmit a first wireless signal including first encrypted authentication information (par. 5 l.33-36).
 - c) A first processor configured to compare stored biometric data with detected biometric data of the first entity and configured to enable or disable use of the first device based on a result of the comparison, and configured to encrypt first authentication information with a first private key into the first encrypted authentication information (par. 5 l.19-21, par. 15 l.34-36, par. 16 l.7-10 and par. 17).
 - d) A first biometric detector for detecting biometric data of the first entity (par. 5 l.21-25).
 - e) A first memory for storing biometric data of the first entity, a private key of the first entity authorized to use the first device, and the first authentication information (par. 5 l.19-21).
- 4 The present application does not meet the criteria of Article 33(1) PCT, because the subject-matter of claim 67 is not new in the sense of Article 33(2) PCT.
Document D3 discloses (the references in parentheses applying to this document):
- a) A first wireless device (par. 30 and par. 54).
 - b) A processor configured to enable operation of the first wireless device if it receives an enablement signal validating first biometric information of a first entity and configured to generate a non-predictable signal from the biometric information (par. 36 The processor generates a non-predictable signal from the biometric data when it encrypts the data.)
 - c) A first wireless transmitter and receiver configured to transmit a first wireless signal including first encrypted biometric information of the first entity and to receive the enablement signal (par. 30, 36 and 39 The enablement signal comes from the authentication server via the ECSP unit in the form of a service).
 - d) A first biometric detector for detecting the first biometric information of the first entity (par. 36).
- 5 Dependent claims 2-40, 42-66, 68-75 do not contain any features which, in

combination with the features of any claim to which they refer, meet the requirements of the PCT in respect of novelty and/or inventive step (Article 33(2) and (3) PCT).

The dependent claims contain features that are part of the common general knowledge like encryption methods, biometric data capture devices and methods for securing communications. These features represent mere implementation details that are well-known to the person skilled in the art, and will not justify an inventive activity.

It is worth to say that the application merely contains a juxtaposition of different techniques used in authentication and cryptography functioning in their normal way and not producing any non-obvious working inter-relationship that justifies an inventive activity.

Possible steps after receipt of the international search report (ISR) and written opinion of the International Searching Authority (WO-ISA)

General information

For all international applications filed on or after 01/01/2004 the competent ISA will establish an ISR. It is accompanied by the WO-ISA. Unlike the former written opinion of the IPEA (Rule 66.2 PCT), the WO-ISA is not meant to be responded to, but to be taken into consideration for further procedural steps. This document explains about the possibilities.

Amending claims under Art. 19 PCT

Within 2 months after the date of mailing of the ISR and the WO-ISA the applicant may file amended claims under Art. 19 PCT directly with the International Bureau of WIPO. The PCT reform of 2004 did not change this procedure. For further information please see Rule 46 PCT as well as form PCT/ISA/220 and the corresponding Notes to form PCT/ISA/220.

Filing a demand for international preliminary examination

In principle, the WO-ISA will be considered as the written opinion of the IPEA. This should, in many cases, make it unnecessary to file a demand for international preliminary examination. If the applicant nevertheless wishes to file a demand this must be done before expiry of 3 months after the date of mailing of the ISR/ WO-ISA or 22 months after priority date, whichever expires later (Rule 54bis PCT). Amendments under Art. 34 PCT can be filed with the IPEA as before, normally at the same time as filing the demand (Rule 66.1 (b) PCT).

If a demand for international preliminary examination is filed and no comments/amendments have been received the WO-ISA will be transformed by the IPEA into an IPRP (International Preliminary Report on Patentability) which would merely reflect the content of the WO-ISA. The demand can still be withdrawn (Art. 37 PCT).

Filing informal comments

After receipt of the ISR/WO-ISA the applicant may file informal comments on the WO-ISA directly with the International Bureau of WIPO. These will be communicated to the designated Offices together with the IPRP (International Preliminary Report on Patentability) at 30 months from the priority date. Please also refer to the next box.

End of the international phase

At the end of the international phase the International Bureau of WIPO will transform the WO-ISA or, if a demand was filed, the written opinion of the IPEA into the IPRP, which will then be transmitted together with possible informal comments to the designated Offices. The IPRP replaces the former IPER (international preliminary examination report).

Relevant PCT Rules and more information

Rule 43 PCT, Rule 43bis PCT, Rule 44 PCT, Rule 44bis PCT, PCT Newsletter 12/2003, OJ 11/2003, OJ 12/2003

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		11768729
	Filing Date		2007-06-26
	First Named Inventor	Kenneth P. Weiss	
	Art Unit		2435
	Examiner Name	B. W. Dada	
	Attorney Docket Number		W0537-700620

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	4720860		1988-01-19	Weiss	
	2	4856062		1989-08-08	Weiss	
	3	4885778		1989-12-05	Weiss	
	4	4998279		1991-03-05	Weiss	
	5	5023908		1991-06-11	Weiss	
	6	5058161		1991-10-15	Weiss	
	7	5097505		1992-03-17	Weiss	
	8	5168520		1992-12-01	Weiss	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		11768729
Filing Date		2007-06-26
First Named Inventor	Kenneth P. Weiss	
Art Unit		2435
Examiner Name	B. W. Dada	
Attorney Docket Number		W0537-700620

9	5237614		1993-08-17	Weiss	
10	5361062		1994-11-01	Weiss et al.	
11	5367572		1994-11-22	Weiss	
12	5398285		1995-03-14	Borgelt et al.	
13	5479512		1995-12-26	Weiss	
14	5485519		1996-01-16	Weiss	
15	5664109		1997-09-02	Johnson et al.	
16	5813006		1998-09-22	Polnerow et al.	
17	5870723		1999-02-09	Pare, Jr. et al.	
18	5915023		1999-06-22	Bernstein	
19	6073106		2000-06-06	Rozen et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		11768729
Filing Date		2007-06-26
First Named Inventor	Kenneth P. Weiss	
Art Unit		2435
Examiner Name	B. W. Dada	
Attorney Docket Number		W0537-700620

	20	6088450		2000-07-11	Davis et al.	
	21	6130621		2000-10-10	Weiss	
	22	6202055		2001-03-13	Houvener et al.	
	23	6253202		2001-06-26	Gilmour	
	24	6253203		2001-06-26	O'Flaherty et al.	
	25	6260039		2001-07-10	Schneck et al.	
	26	6308203		2001-10-23	Itabashi et al.	
	27	6309342		2001-10-30	Blazey et al.	
	28	6393421		2002-05-21	Paglin	
	29	6516315		2003-02-04	Gupta	
	30	6546005		2003-04-08	Berkley et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		11768729
Filing Date		2007-06-26
First Named Inventor	Kenneth P. Weiss	
Art Unit		2435
Examiner Name	B. W. Dada	
Attorney Docket Number		W0537-700620

31	6581059		2003-06-17	Barrett et al.	
32	6640211		2003-10-28	Holden	
33	6658400		2003-12-02	Perell et al.	
34	6819219		2004-11-16	Bolle et al.	
35	6845448		2005-01-18	Chaganti et al.	
36	6941271		2005-09-06	Soong	
37	7007298		2006-02-28	Shinzaki et al.	
38	7249112		2007-07-24	Berardi et al.	
39	7278026		2007-10-02	McGowan	
40	7412604		2008-08-12	Doyle	
41	7489781		2009-02-10	Klassen et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	11768729
Filing Date	2007-06-26
First Named Inventor	Kenneth P. Weiss
Art Unit	2435
Examiner Name	B. W. Dada
Attorney Docket Number	W0537-700620

42	7502459		2009-03-10	Moseley	
43	7548981		2009-06-16	Taylor et al.	
44	7552333		2009-06-23	Wheeler et al.	
45	7571139		2009-08-04	Giordano et al.	
46	7657639		2010-02-02	Hinton	
47	7705732		2010-04-27	Bishop et al.	
48	8079079		2011-12-13	Zhang et al.	

If you wish to add additional U.S. Patent citation information please click the Add button.

[Add](#)

U.S.PATENT APPLICATION PUBLICATIONS

[Remove](#)

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	20010032100		2001-10-18	Mahmud et al.	
	2	20010044900		2001-11-22	Uchida	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	11768729
Filing Date	2007-06-26
First Named Inventor	Kenneth P. Weiss
Art Unit	2435
Examiner Name	B. W. Dada
Attorney Docket Number	W0537-700620

3	20020046061		2002-04-18	Wright et al.	
4	20020090930		2002-07-11	Fujiwara et al.	
5	20020176610		2002-11-28	Okazaki et al.	
6	20020178364		2002-11-28	Weiss	
7	20030014372		2003-01-16	Wheeler et al.	
8	20030115490		2003-06-19	Russo et al.	
9	20030123713		2003-07-03	Geng	
10	20030129965		2003-07-10	Siegel	
11	20030163710		2003-08-28	Ortiz et al.	
12	20030226041		2003-12-04	Palmer et al.	
13	20040017934		2004-01-29	Kocher	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		11768729
Filing Date		2007-06-26
First Named Inventor	Kenneth P. Weiss	
Art Unit		2435
Examiner Name	B. W. Dada	
Attorney Docket Number		W0537-700620

14	20040034771		2004-02-19	Edgett et al.	
15	20040059923		2004-03-25	ShamRao	
16	20040111625		2004-06-10	Duffy et al.	
17	20040117215		2004-06-17	Marchosky	
18	20040117302		2004-06-17	Weichert et al.	
19	20040133787		2004-07-08	Doughty et al.	
20	20040151351		2004-08-05	Ito	
21	20040188519		2004-09-30	Cassone	
22	20040236699		2004-11-25	Beenau et al.	
23	20050001711		2005-01-06	Doughty et al.	
24	20050039027		2005-02-17	Shapiro	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		11768729
Filing Date		2007-06-26
First Named Inventor	Kenneth P. Weiss	
Art Unit		2435
Examiner Name	B. W. Dada	
Attorney Docket Number		W0537-700620

25	20050187843		2005-08-25	Lapsley et al.	
26	20050187873		2005-08-25	Labrou et al.	
27	20050210270		2005-09-22	Rohatgi et al.	
28	20050235148		2005-10-20	Scheidt et al.	
29	20050238208		2005-10-27	Sim	
30	20060000900		2006-01-05	Fernandes et al.	
31	20060016884		2006-01-26	Block et al.	
32	20060104486		2006-05-18	Le Saint et al.	
33	20060122939		2006-06-08	Cohen et al.	
34	20060165060		2006-07-27	Dua	
35	20060206724		2006-09-14	Schaufele et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		11768729
Filing Date		2007-06-26
First Named Inventor	Kenneth P. Weiss	
Art Unit		2435
Examiner Name	B. W. Dada	
Attorney Docket Number		W0537-700620

	36	20060256961		2006-11-16	Brainard et al.	
	37	20070005988		2007-01-04	Zhang et al.	
	38	20070040017		2007-02-22	Kozlay	
	39	20070079136		2007-04-05	Vishik et al.	
	40	20070124597		2007-05-31	Bedingfield	
	41	20070124697		2007-05-31	Dongelmans	
	42	20070140145		2007-06-21	Kumar et al.	
	43	20070186105		2007-08-09	Bailey et al.	
	44	20070186115		2007-08-09	GAO et al.	
	45	20070198436		2007-08-23	Weiss	
	46	20070245152		2007-10-18	Pizano et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		11768729
Filing Date		2007-06-26
First Named Inventor	Kenneth P. Weiss	
Art Unit		2435
Examiner Name	B. W. Dada	
Attorney Docket Number		W0537-700620

47	20080005576		2008-01-03	Weiss	
48	20080021997		2008-01-24	HINTON	
49	20080040274		2008-02-14	UZO	
50	20080127311		2008-05-29	Yasaki et al.	
51	20080212848		2008-09-04	Doyle	
52	20080275819		2008-11-06	Rifai	
53	20090083544		2009-03-26	Scholnick et al.	
54	20090144814		2009-06-04	Sacco	
55	20090175507		2009-07-09	Schaffner	
56	20090203355		2009-08-13	Clark	
57	20100046443		2010-02-25	Jia et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	11768729
Filing Date	2007-06-26
First Named Inventor	Kenneth P. Weiss
Art Unit	2435
Examiner Name	B. W. Dada
Attorney Docket Number	W0537-700620

58	20120130904		2012-05-24	Weiss	
59	20120240195		2012-09-20	Weiss	

If you wish to add additional U.S. Published Application citation information please click the Add button. [Add](#)

FOREIGN PATENT DOCUMENTS

[Remove](#)

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² j	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	0986209	EP	A2	2000-03-15	Mitsubishi Electric Corp		<input type="checkbox"/>
	2	1081632	EP	A1	2001-03-07	Keyware, Technologies		<input type="checkbox"/>
	3	2382006	GB	A	2003-05-14	Ibm		<input type="checkbox"/>
	4	0214985	WO	A2	2002-02-21	Kern, Daniel		<input type="checkbox"/>
	5	1992007436	WO	A1	1992-04-30	Security Dynamics Techn		<input type="checkbox"/>
	6	1996036934	WO	A1	1996-11-21	Smart Touch L L C		<input type="checkbox"/>
	7	2012037479	WO	A1	2012-03-22	Universal Secure Registry, Llc		<input type="checkbox"/>

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		11768729	
	Filing Date		2007-06-26	
	First Named Inventor	Kenneth P. Weiss		
	Art Unit		2435	
	Examiner Name	B. W. Dada		
	Attorney Docket Number		W0537-700620	

	8	9207436	WO	A1	1992-04-30	Security Dynamics Technologies, Inc	<input type="checkbox"/>
--	---	---------	----	----	------------	-------------------------------------	--------------------------

If you wish to add additional Foreign Patent Document citation information please click the Add button **Add**

NON-PATENT LITERATURE DOCUMENTS

Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	"Information Security: Challenges in Using Biometrics" 9 September 2003. All pages. < http://www.gao.gov/new.items/d031137t.pdf >	<input type="checkbox"/>
	2	International Search Report from PCT/US2007/070701 mailed March 11, 2008	<input type="checkbox"/>

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature		Date Considered	
--------------------	--	-----------------	--

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	11768729		
Filing Date	2007-06-26		
First Named Inventor	Kenneth P. Weiss		
Art Unit	2435		
Examiner Name	B. W. Dada		
Attorney Docket Number	W0537-700620		

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

See attached certification statement.

The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.

A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Matthew H. Grady/	Date (YYYY-MM-DD)	2014-03-28
Name/Print	Matthew H. Grady	Registration Number	52957

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.



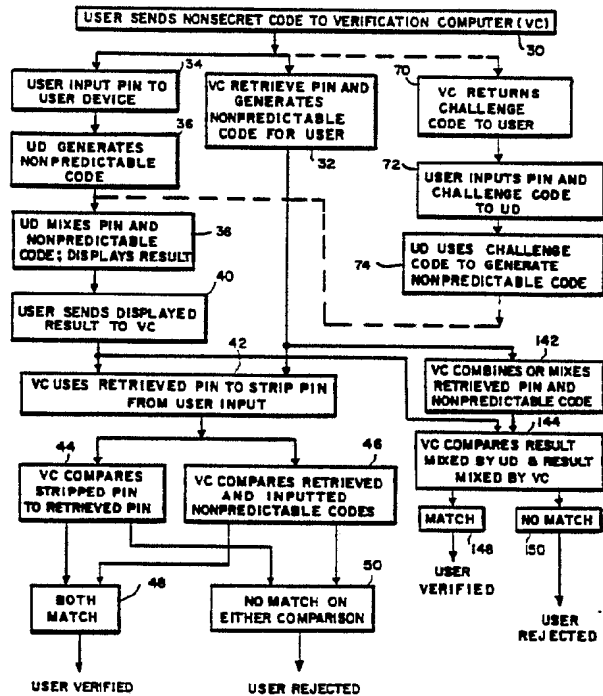
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification ⁵ : H04K 1/00</p>	<p>A1</p>	<p>(11) International Publication Number: WO 92/07436 (43) International Publication Date: 30 April 1992 (30.04.92)</p>
<p>(21) International Application Number: PCT/US91/03034 (22) International Filing Date: 30 April 1991 (30.04.91) (30) Priority data: 597,784 19 October 1990 (19.10.90) US 670,705 18 March 1991 (18.03.91) US (71) Applicant: SECURITY DYNAMICS TECHNOLOGIES, INC. [US/US]; One Alewife Center, Cambridge, MA 02140-2312 (US). (72) Inventor: WEISS, Kenneth, P. ; 7 Park Avenue, Newton, MA 02159 (US). (74) Agent: OLIVERIO, M., Lawrence; Wolf, Greenfield & Sacks, Federal Reserve Plaza, 600 Atlantic Avenue, Boston, MA 02210 (US).</p>		<p>(81) Designated States: AT (European patent), AU, BE (European patent), CA, CH (European patent), DE (European patent), DK (European patent), ES (European patent), FR (European patent), GB (European patent), GR (European patent), IT (European patent), JP, LU (European patent), NL (European patent), SE (European patent). Published <i>With international search report.</i></p>

(54) Title: METHOD AND APPARATUS FOR PERSONAL IDENTIFICATION

(57) Abstract

A method and apparatus for providing improved security for a personal identification number (PIN) in a personal identification and verification system of the type wherein a time dependent nonpredictable code is generated at a device in the possession of the individual (36), which code is unique to the individual and this code is communicated to, and compared with a nonpredictable code generated at a central verification computer (46). In this system, the PIN is mixed with the nonpredictable code before transmission of these values to the central verification computer (38). A nonsecret code (30) is previously transmitted to the central verification computer and is used by the verification computer to retrieve the PIN and independently generate the time dependent appropriate nonpredictable code for the user (74). These retrieved PIN and generated code values are used by the verification computer either (a) to strip the PIN from the transmitted nonpredictable code (42) and the stripped PIN and remaining nonpredictable code are compared with the corresponding retrieved values in order to determine verification (44, 46); or (b) to be mixed and then compared with the mixed PIN and code which is transmitted to the verification computer (144).



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	ES	Spain	MG	Madagascar
AU	Australia	FI	Finland	ML	Mali
BB	Barbados	FR	France	MN	Mongolia
BE	Belgium	GA	Gabon	MR	Mauritania
BF	Burkina Faso	GB	United Kingdom	MW	Malawi
BG	Bulgaria	GN	Guinea	NL	Netherlands
BJ	Benin	GR	Greece	NO	Norway
BR	Brazil	HU	Hungary	PL	Poland
CA	Canada	IT	Italy	RO	Romania
CF	Central African Republic	JP	Japan	SD	Sudan
CG	Congo	KP	Democratic People's Republic of Korea	SE	Sweden
CH	Switzerland	KR	Republic of Korea	SN	Senegal
CI	Côte d'Ivoire	LI	Liechtenstein	SU⁺	Soviet Union
CM	Cameroon	LK	Sri Lanka	TD	Chad
CS	Czechoslovakia	LU	Luxembourg	TG	Togo
DE⁺	Germany	MC	Monaco	US	United States of America
DK	Denmark				

+ Any designation of "SU" has effect in the Russian Federation. It is not yet known whether any such designation has effect in other States of the former Soviet Union.

- 1 -

METHOD AND APPARATUS FOR PERSONAL IDENTIFICATIONCross Reference to Other Applications

5 This application is a continuation-in-part of application serial no. 07/341,932 filed April 21, 1989, which is a continuation-in-part of application serial no. 802,579 filed November 27, 1985, issued December 5, 1989 as U.S. Patent No. 4,885,778, which application is itself a continuation-in-part of application serial no. 676,626 filed November 30, 1984, now U.S. Patent No. 4,720,860, issued January 10 19, 1988. The disclosures and specifications of all of the foregoing applications/patents are incorporated herein by reference as if fully set forth.

- 2 -

Field of the Invention

This invention relates to methods and apparatus for identifying an individual and more particularly to methods and apparatus for providing improved security for a personal identification number (PIN) utilized in conjunction with such an identification system.

Background of the Invention

Personal identification systems may be based on something someone has, such as a card or badge, something that someone knows, such as a PIN, or some characteristic of the individual, such as his fingerprints or speech pattern. Security for such systems is enhanced by utilizing two or more of the above in performing the identification.

For example, parent Patent No. 4,720,860, discloses a personal identification system wherein the individual has a card or other small, portable device which contains a microprocessor programmed to utilize a secret algorithm to generate a nonpredictable number from a stored value unique to the individual and a time varying value provided for example by a clock. The nonpredictable value is preferably displayed on the device. The individual then enters his secret PIN into a central verification system, either directly or over a telephone line, causing the central system to access

- 3 -

stored information corresponding to the individual
and to utilize at least some of this information to
generate a nonpredictable value at the central
computer utilizing the same algorithm as at the
5 individual's microprocessor. At the same time this
is being done, the individual is entering the number
appearing at that period of time on the display of
his device. The two values will match, signifying
identification of the individual, only if the
10 individual has entered the correct PIN and if the
individual has the proper device so that the
nonpredictable code displayed corresponds to that
being generated at the central verification computer.

In other systems, such as those shown in U.S.
15 Patent No. 4,599,489 issued July 8, 1986, the PIN
may either be stored in the user's device, or may be
entered by the user. If the PIN is stored in the
device, it is read from the device by a suitable
reader and causes the central verification computer
20 to generate a unique challenge code to the
individual. This challenge code may either be
entered by the individual into his machine, or may
be automatically sensed by the machine, and is
operated on by the user's device to generate a
25 unique nonpredictable code which is then entered
into the central computer to effect verification.

One potential difficulty with either of the
systems indicated above is that an unauthorized

- 4 -

individual may be able to obtain access to the user's PIN by electronic eavesdropping, reducing the security provided by the system. If, for example, the PIN is transmitted over public lines, such as
5 telephone lines, from the user to the central verification computer, it may be possible to tap these lines and intercept the PIN as it is being transmitted. If the PIN is stored in the device, someone obtaining the device surreptitiously may,
10 through sophisticated means, be able to determine the PIN stored in the device and thus defeat the security of the system. Furthermore, any storing of a PIN or password in the portable device for comparison defeats the purpose of an independent
15 identification factor and reduces security to a "thing" possessed.

A need therefore exists for an improved means of communicating a PIN or other user identification code to a central verification system such that
20 someone tapping the line over which the code is being sent will be unable to determine the secret identification number and someone obtaining possession of the user device will also not be able to obtain access to the user's secret identification
25 number from the device.

- 5 -

Summary of the Invention

In accordance with the above, this invention provides a method for personal identification and apparatus for the practice thereof wherein a device
5 in the possession of the individual is utilized to generate a unique, time varying, nonpredictable code; the nonpredictable code generated at a given time is mixed with a secret PIN for the individual; the mixed output is communicated to a central
10 verification computer; and the verification computer typically strips the PIN from the communicated value and utilizes the stripped PIN and remaining nonpredictable code to perform a verification operation. Alternatively and equivalently, the
15 mixed output which is communicated to the verification computer may be verified in the verification computer without stripping of the PIN. Preferably, before the mixed value is communicated to the verification computer, a nonsecret
20 identifying code for the individual is communicated to the verification computer; the verification computer utilizes the nonsecret identifying code to obtain the PIN and appropriate nonpredictable code for the individual; and the verification operation
25 includes the PIN and appropriate nonpredictable code obtained during the obtaining step being compared with the stripped PIN and remaining nonpredictable code. Alternatively the PIN may not be stripped

- 6 -

from the mixed value, the verification computer may utilize the nonsecret identifying code to retrieve or obtain the PIN and appropriate nonpredictable code, combine the retrieved PIN and appropriate nonpredictable code, and perform a verification operation between the mixed value communicated to the verification computer and the combination of the retrieved PIN and appropriate nonpredictable code. The verification computer may also generate a unique challenge value in response to the nonsecret identifying code which challenge code is communicated to the device in possession of the individual. For one embodiment, the challenge code is communicated to the individual and the individual inputs the challenge value and the PIN to his device, the device includes means responsive to the challenge value for generating the nonpredictable code. During the mixing step, the device may receive the PIN and the nonpredictable code and generate an output which is a predetermined function of the inputs. The predetermined function may, for example, be a sum of the inputs, for example the sum of the inputs without carry.

The foregoing and other objects, features and advantages of the invention will be apparent from the following more particular description of preferred embodiments of the invention as illustrated in the accompanying drawings.

- 7 -

In the Drawings

Fig. 1 is a semi-block schematic diagram of the verification system of a first embodiment of the invention.

5 Fig. 2 is a block schematic diagram of a second embodiment of the invention.

Fig. 3 is a block flow diagram illustrating the operation of the first embodiment of the invention and alternative steps for the second embodiment of the invention.

10

Detailed Description

Fig. 1 shows illustrative structure for a personal identification system of a first embodiment of the invention. In this figure, a user

15 verification device 10 is provided which is of the type described in the parent applications. The device is preferably of the general size and shape of a standard credit card, although its thickness dimension may be slightly greater than that of such

20 cards. The device 10 has a clock which generates a time-dependent digital output to a microprocessor which is programmed with a unique algorithm to operate on the time-dependent clock input and on a stored static value unique to a given user to

25 generate a multi-bit nonpredictable code. A plurality of input areas 12 are provided on the face of device 10. These areas are preferably each

- 8 -

indicative of a numerical digit, for example the digits 1 - 0 as shown in Fig. 1, and may be pressure-sensitive pads or otherwise adapted to generate an electrical output indicative of the area when the area is touched by the user. Spacing may be provided between the individual areas 12 to assure distinctive outputs. As will be described in greater detail hereinafter, the user may input his unique PIN on areas 12 which are mixed in the processor in device 10 with the nonpredictable code generated therein in response to the time-dependent and static inputs to generate a multi-bit nonpredictable code which is displayed on area 14 of device 10. Area 14 may be a liquid crystal display or other suitable display device for producing numeric or alpha-numeric characters. Each area of display 14 is adapted to display a different digit of the nonpredictable code.

The user initially transmits a nonsecret identifying code to verification computer 16 by keying this number into a telephone 18 at his location. This number is transmitted over telephone lines 20 to telephone 22 at the verification station and through a modem 24 at this station to the verification computer. The user may then use the telephone 18 to key in and transmit the nonpredictable code being displayed at that time on display 14.

- 9 -

Fig. 3 is a flow diagram illustrating in greater detail the operation of the system of Fig. 1 to perform a verification operation. Referring to Fig. 3, the first step in the operation, step 30, is for the user to send his nonsecret code to verification computer (VC) 16. As previously indicated, this is accomplished by the user keying his nonsecret identification number into telephone 18 for transmission through telephone line 20, telephone 22 and modem 24 to the verification computer.

In response to the user input of his nonsecret code, the verification computer retrieves the user's PIN and generates the nonpredictable code for the user, using the same algorithm and stored static value as user device 10, and using a time-related value from a clock device at the verification computer, which is maintained in synchronism with the clock at the user device in a manner discussed in the parent application (step 32). At the same time that the verification computer is retrieving the PIN and nonpredictable code for the user, the user is inputting his PIN into his device 10 using key pads or areas 12 (step 34). While the user is inputting his pin, the user device is continuously generating nonpredictable code values at its internal processor in response to the clock value and the stored static value using the unique algorithm at the user device processor (step 36).

- 10 -

The next step in the operation, step 38, is for the generated nonpredictable code and the inputted pin to be mixed by the processor in device 10 to generate a new nonpredictable code which is
5 displayed on display 14. The mixing operation may be a simple addition of the two values without carry, or with carry, (a constant added to a pseudo random number produces a pseudo random number) or may involve a more sophisticated mixing algorithm.

10 During step 40, the user transmits the displayed value by use of telephone 18 through telephone line 20, telephone 22, and modem 24 to verification computer 16.

15 During the next step in the operation, step 42, the verification computer uses the PIN for the user which was retrieved during step 32 to strip the PIN from the inputted nonpredictable code, the result being a PIN value and a nonpredictable code value. During step 44 the stripped PIN is compared with the
20 PIN retrieved during step 32 and during step 46 the nonpredictable code remaining after the inputted value has the PIN stripped therefrom is compared with the retrieved nonpredictable code. If matches are obtained during both steps 44 and 46 (step 48)
25 the verification computer signifies verification. If a match is not found during either step 44 or step 46 (step 50) then the user is rejected.

- 11 -

Alternatively to steps 42, 44, 46, 48 and 50, the PIN and nonpredictable code which are retrieved in step 32 may be combined or mixed by the verification computer during step 142 according to the same mixing operation which was carried out by the processor or user device 10 in step 38, e.g. by a simple addition of the two values without carry, with carry, or according to some other more sophisticated algorithm. During alternative step 144 the separate results of the mixing operations carried out by the user device 10 and the verification computer 16 are compared. If a match is obtained, step 148, the user is verified. If a match is not found, step 150, the user is rejected.

A procedure is thus provided wherein user verification may be obtained using the simple and inexpensive procedure disclosed in the parent applications while still providing a high level of security for the user PIN. This security is achieved since the user PIN is never available on an open line which could be tapped except in the form of a word which is a mixture of the PIN with a nonpredictable code and which is virtually impossible to decipher.

Fig. 2 illustrates an alternative configuration in which the teachings of this invention may be utilized. In Fig. 2, the user device 10 is of the same type shown in Fig. 1. However, for this

- 12 -

embodiment of the invention, the user device is adapted to be used in proximity to the verification station rather than from a remote location over telephone lines. For this embodiment of the invention, the verification station 60 includes a computer 62, a display 64, such as for example a CRT display, and an input device 66 which may, for example, be a standard computer input keyboard. Referring again to Fig. 3, the operation with this embodiment of the invention starts with step 30, during which the user sends a nonsecret code to the verification computer 62 by, for example, keying this code into input device 66. In response to receiving the nonsecret code, computer 60 retrieves the PIN and generates the nonpredictable code for the user (step 32) and also retrieves a challenge code for the user which is displayed on display 64 (step 70). The user inputs his PIN and the challenge code in an order established for the system to user device 10 using input pads 12 (step 72). During step 74, the processor in device 10 uses the inputted challenge code and the time inputted from its clock to generate a nonpredictable code which, during step 38, is mixed with the inputted pin and the results are displayed on display 14 of device 10. From this point on, the operation for this embodiment of the invention is the same as that previously described with respect to the embodiment of Fig. 1.

- 13 -

Thus, with this embodiment of the invention, as with the prior embodiment of the invention, the pin in uncoded form is never transmitted in a manner such that it could be observed and is not resident in the user's device where it might, using sophisticated technology, be retrieved.

As an alternative to the embodiment shown in Fig. 2, the nonsecret code may be recorded in machine-readable form on device 10 and input device 66 might include a card reader which the card is inserted into to permit the nonsecret code to be read into computer 62.

While the invention has been shown and described above with reference to preferred embodiments, the foregoing and other changes in form and detail may be made therein by one skilled in the art without departing from the spirit and scope of the invention.

What is claimed is:

- 14 -

CLAIMS

1. In a personal identification system of the type wherein a user is provided with a device generating a unique, time-varying, nonpredictable code, with a nonsecret identifying code and with a secret PIN, the nonpredictable code at a given instant and the PIN being provided to a central verification computer to effect verification; apparatus for providing improved security for the PIN comprising:

means for mixing the nonpredictable code generated by the device at a given time with the PIN according to a predetermined algorithm to generate a combined coded value;

means for separately communicating the nonsecret identifying code and the combined coded value to the central verification computer; and

wherein the central verification computer includes means for utilizing the nonsecret identifying code to retrieve the PIN and generate an appropriate, unique, time varying nonpredictable code for the individual, and at least one of:

(a) a means for utilizing the retrieved PIN, appropriate nonpredictable code and the combined coded value in performing a verification operation; or

- 15 -

(b) a means for stripping the PIN from the combined coded value received from the means for communicating, the nonpredictable code remaining after stripping of the PIN and means for utilizing the retrieved PIN, and appropriate nonpredictable code for performing a verification operation.

2. Apparatus as claimed in claim 1 including means operative prior to the communicating of the value from the mixing means for communicating the nonsecret identifying code to said verification computer.

3. Apparatus as claimed in claim 2 wherein said verification computer includes means for utilizing the communicated nonsecret identifying code to retrieve the PIN and a unique challenge value for the individual; and
means for communicating the challenge value to the device.

4. Apparatus as claimed in claim 3 wherein said challenge value communicating means includes means for communicating the challenge value to the individual; and
wherein the device includes means for permitting the individual to input the challenge value and his PIN to the device.

- 16 -

5. Apparatus as claimed in claim 4 wherein said device includes means responsive to the challenge value for generating the nonpredictable code; and

5 wherein said mixing means includes means, included as part of the device, for receiving the inputted PIN and the generated nonpredictable value and for generating an output which is a predetermined function of the input.

10 6. Apparatus as claimed in claim 5 wherein said mixing means adds the PIN to the nonpredictable code.

7. Apparatus as claimed in claim 1 wherein said device includes means for permitting the individual to input his PIN to the device; and

15 wherein said means for mixing is included as part of said device and is adapted to receive the PIN inputted by the individual and the nonpredictable code and to generate an output which

20 is a predetermined function of the input.

8. Apparatus as claimed in claim 7 wherein said mixing means adds the PIN to the nonpredictable code.

- 17 -

5 9. Apparatus as claimed in claim 1 wherein said verification computer includes a means for mixing the retrieved PIN and appropriate nonpredictable code generated by the verification computer at a given time according to the predetermined algorithm to generate a second combined coded value.

10 10. Apparatus as claimed in claim 9 wherein the verification operation comprises comparing the combined coded value with the second combined coded value.

15 11. Apparatus as claimed in claim 1 wherein the means for performing a verification operation includes means for comparing the PIN and nonpredictable code obtained in response to the nonsecret identifying code with the stripped PIN and remaining nonpredictable code.

20 12. A method for identifying an individual comprising the steps of:
utilizing a device in the possession of the individual to generate a unique time-varying, nonpredictable code;
25 mixing the nonpredictable code generated at a given time with a secret PIN for the individual to generate a combined code; and

- 18 -

communicating a nonsecret identifying code for the individual and the combined code to a central verification computer;

5 the verification computer utilizing the nonsecret identifying code to retrieve the PIN and generate an appropriate, unique, time-varying nonpredictable code for the individual, and at least one of:

- 10 (a) utilizing the retrieved PIN, appropriate nonpredictable code, and the combined code to perform a verification operation; or
- (b) stripping the PIN from the communicated combined code and utilizing the retrieved PIN and nonpredictable code, the stripped
- 15 PIN and the remaining nonpredictable code to perform a verification operation.

13. A method as claimed in claim 12 wherein the verification

20 computer also generates a unique challenge value in response to the nonsecret identifying code; and including the step of communicating the challenge value to the device in possession of the individual.

14. A method as claimed in claim 13 wherein the

25 challenge value is communicated to the individual; and

- 19 -

including the step of the individual inputting the challenge value and his PIN to the device.

5 15. A method as claimed in claim 14 wherein the device includes means responsive to the challenge value for generating the nonpredictable code; and
wherein the mixing step includes the device receiving the PIN and the nonpredictable code and generating an output which is a predetermined
10 function of the inputs.

16. A method as claimed in claim 15 wherein said predetermined function is a sum of said inputs.

15 17. A method as claimed in claim 15 including the step of the individual inputting his PIN to the device; and
wherein the mixing step includes the device receiving the PIN inputted by the individual and the nonpredictable code and generating an output which is a predetermined function of the inputs.

20 18. A method as claimed in claim 17 wherein said predetermined function is a sum of said input.

19. A method as claimed in claim 12 wherein the verification computer utilizes the retrieved PIN and

- 20 -

appropriate nonpredictable code by combining them to obtain a second combined code.

20. A method as claimed in claim 19 wherein the verification operation comprises comparing the
5 combined code and the second combined code.

21. A method as claimed in claim 12 wherein the verification operation includes comparing the retrieved PIN and the nonpredictable code generated by the verification computer with the stripped PIN
10 and the remaining nonpredictable code.

1/2

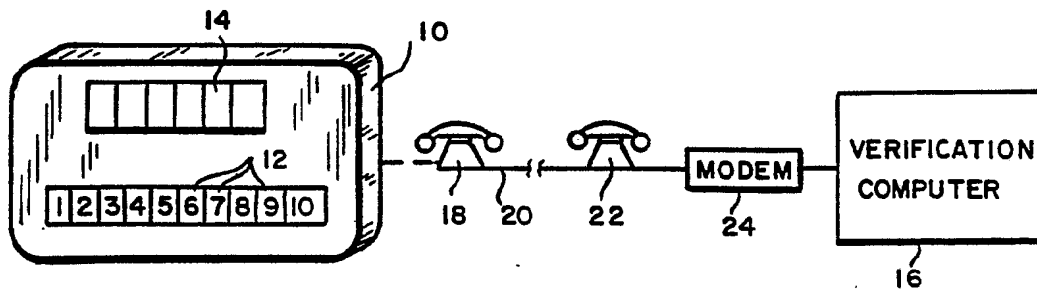


FIG. 1

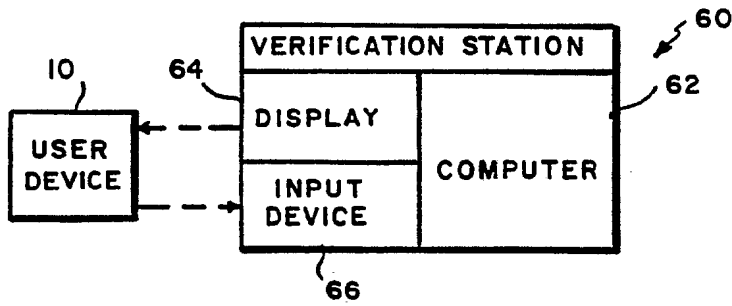


FIG. 2

2/2

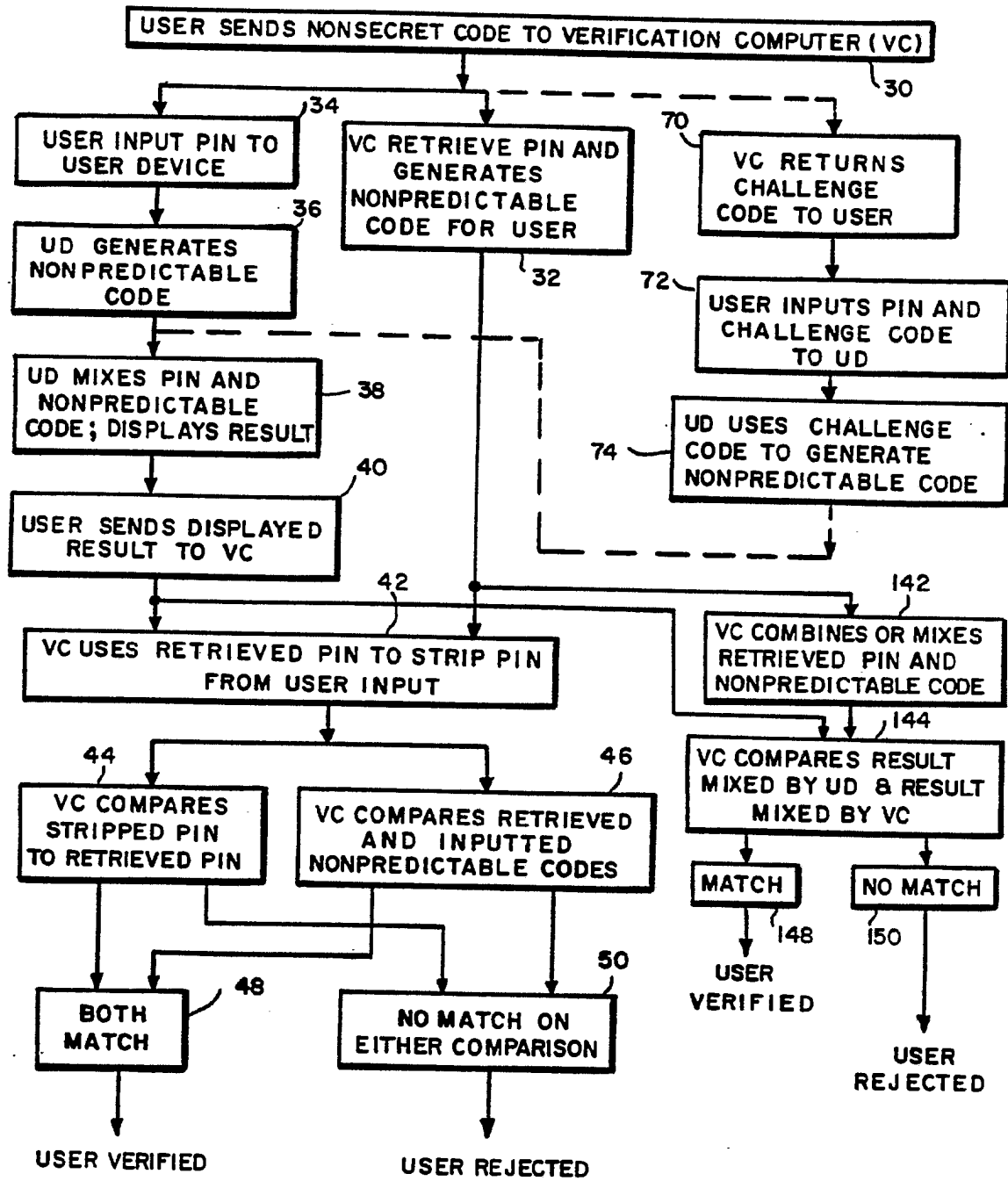
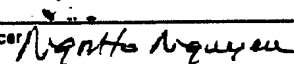


FIG.3

INTERNATIONAL SEARCH REPORT

International Application No. PCT/US91/03034

I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) ⁶		
According to International Patent Classification (IPC) or to both National Classification and IPC		
IPC(5) H04K 1/00 US 380/23, 25		
II. FIELDS SEARCHED		
Minimum Documentation Searched ⁷		
Classification System	Classification Symbols	
US	380/23, 24, 25, 28, 48	
Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched ⁸		
III. DOCUMENTS CONSIDERED TO BE RELEVANT ⁹		
Category ⁹	Citation of Document, ¹¹ with indication, where appropriate, of the relevant passages ¹²	Relevant to Claim No. ¹³
X	US,A 4,720,860 (WEISS) 19 January 1988	1-21
A	US,A 4,890,323 (BEKER ET AL) 26 December 1989	1-21
A	US,A 4,885,778 (WEISS) 05 December 1989	1-21
A	US,A 4,856,062 (WEISS) 08 August 1989	1-21
A	US,A 4,819,267 (CARGILE ET AL) 04 April 1989	1-21
A	US,A 4,802,216 (IRWIN ET AL) 31 January 1989	1-21
A	US,A 4,731,841 (ROSEN ET AL) 15 March 1988	1-21
A	US,A 4,599,489 (CARGILE) 08 July 1986	1-21
A	US,A 4,578,530 (ZEIDLER) 25 March 1986	1-21
A	US,A 4,509,093 (STELLBERGER) 02 April 1985	1-21
<p>⁹ Special categories of cited documents: ¹⁰</p> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier document but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p> <p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.</p> <p>"&" document member of the same patent family</p>		
IV. CERTIFICATION		
Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report	
21 August 1991	27 SEP 1991	
International Searching Authority	Signature of Authorized Officer	
ISA/US	 NGUYEN NGOC-HO INTERNATIONAL DIVISION	
	David Cain	

CORRECTED VERSION

(19) World Intellectual Property Organization International Bureau



(10) International Publication Number WO 2012/037479 A9

(43) International Publication Date 22 March 2012 (22.03.2012)

WIPO | PCT

- (51) International Patent Classification: H04L 29/06 (2006.01) H04W 12/06 (2009.01)
(21) International Application Number: PCT/US2011/051966
(22) International Filing Date: 16 September 2011 (16.09.2011)
(25) Filing Language: English
(26) Publication Language: English
(30) Priority Data: 61/384,146 17 September 2010 (17.09.2010) US; 61/447,497 28 February 2011 (28.02.2011) US; 61/499,961 22 June 2011 (22.06.2011) US
(71) Applicant: UNIVERSAL SECURE REGISTRY, LLC [US/US]; 59 Sargent Street, Newton, MA 02458 (US).
(72) Inventor: and
(75) Inventor/Applicant: WEISS, Kenneth, P. [US/US]; 50 Sargent Street, Newton, MA 02458 (US).
(74) Agent: DONAHOE, Robert, V.; Lando & Anastasi LLP, Riverfront Office Park, One Main Street-suite 1100, Cambridge, MA 02142 (US).
(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ,

CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LR, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Declarations under Rule 4.17:

- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))
as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))

Published:

- with international search report (Art. 21(3))
with amended claims (Art. 19(1))

[Continued on next page]

(54) Title: APPARATUS, SYSTEM AND METHOD EMPLOYING A WIRELESS USER-DEVICE

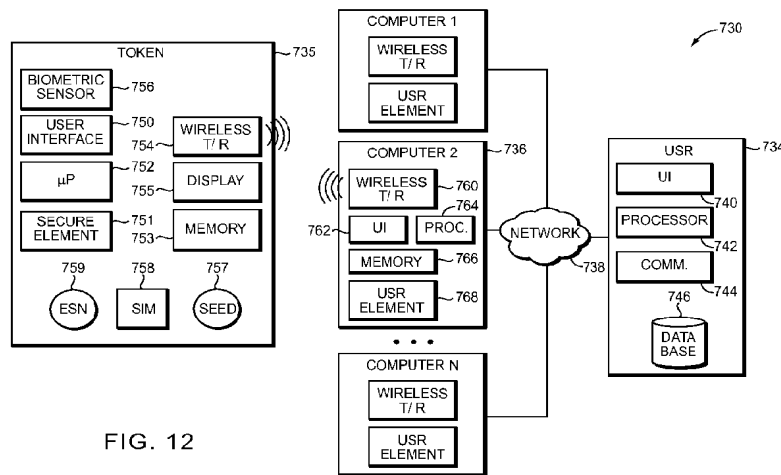


FIG. 12

(57) Abstract: Embodiments of the invention generally relate to apparatus, systems and methods for authentication, in particular, apparatus, systems and methods for authenticating an entity for computer and/or network security, secure authorization of a payment or for funds transfer and for selectively granting privileges and providing other services in response to such authentications. In addition, embodiments of the invention relate generally to apparatus, systems and methods for the communication of information between a mobile user-device and a point-of-sale device to securely provide authorization for a financial transaction.

WO 2012/037479 A9

(48) Date of publication of this corrected version:
26 July 2012

(15) Information about Correction:
see Notice of 26 July 2012

- 1 -

APPARATUS, SYSTEM AND METHOD EMPLOYING A WIRELESS USER-DEVICE

5 RELATED APPLICATIONS

This application claims priority under 35 U.S.C. § 119(e) to each of the following co-
pending U.S. Provisional Applications: Serial No. 61/384,146, entitled "APPARATUS,
SYSTEM AND METHOD FOR SECURE PAYMENT," filed on September 17, 2010; U.S.
Provisional Application Serial No. 61/447,497, entitled "APPARATUS, SYSTEM AND
10 METHOD EMPLOYING A WIRELESS USER-DEVICE," filed on February 28, 2011 and
U.S. Provisional Application Serial No. 61/499,961, entitled "APPARATUS, SYSTEM AND
METHOD FOR EMPLOYING A WIRELESS USER-DEVICE," filed on June 22, 2011, each
of which are incorporated herein by reference in their entirety.

15 BACKGROUND

1. Field of Invention

Embodiments of the invention generally relate to apparatus, systems and methods for
identification, in particular, apparatus, systems and methods for identifying an entity for
20 computer and/or network security, secure authorization of a payment or for funds transfer and
for selectively granting privileges and providing other services in response to such
identifications. In addition, embodiments of the invention relate generally to apparatus,
systems and methods for the communication of information between a mobile user-device and
a point-of-sale device to securely provide authorization for a financial transaction.

25

2. Discussion of Related Art

Millions of financial transactions are conducted daily using electronic systems. Many
of these are conducted using traditional magnetic stripe readers while others are conducted

- 2 -

using smart-cards, mobile phones or other handheld electronic devices. However, these prior approaches all require that an account number (bank account number, credit card account number, debit card account number, etc.) be provided to authorize the transaction. Because a thief with access to an account number poses a significant financial risk and risk of identity theft, financial service providers go to great efforts to try to communicate the account numbers securely when conducting these transactions.

In addition, electronic transactions often require that a user provide information that uniquely identifies the user to allow financial information or other personal information to be used in completing the transaction. This user-identification is generally static-information, that is, the information does not change over time, for example, user names and/or passwords. In addition, the user-identification information uniquely identifies the user. As a result of the well documented risk posed by identity theft, business entities spend enormous amounts of time, effort and money to protect this static user-identity information. The approaches implemented by business entities include using secure networks to transmit the user-identity information, and alternatively or in combination with the preceding, using various forms of encryption to protect the user-identity information from electronic-eavesdroppers. Regardless, each of these prior approach results in the transmission of the highly-sensitive user-identity information.

Further, traditional approaches to identity authentication rely on a verification process. That is, the authenticator receives static user-identity information along with other information such as a time(or event)-varying code. The authenticator employs the user-identity information to establish the user that the entity purports to be. The authenticator then employs the other information to determine whether that information authenticates that the entity is who they purport to be. Such approaches can include multi-factor authentication in which the entity provides the authenticator with information including evidence of one or more of something the user is (for example, a biometric), something the user knows (for example, a PIN); or something the user possesses (for example, a token). In this example, static information (for example, a user name or password) is used to verify the identity of the user to locate the other information (for example, any of biometric data, the user's PIN and/or a seed associated with

- 3 -

the token) concerning the user which is stored by the authenticator. With a proprietary algorithm and the current time, the authenticator generates a non-predictable code using the other information that is associated with the user. The authenticator then determines whether the time-varying code received from the user is the same as that generated by the authenticator.

5 That is, some existing token technologies use a verification process that requires the user to supply a remote authentication system with a unique static index such as a user name or email address. This static information is used to retrieve the user's file, including a secret seed. With a proprietary algorithm and current time, that seed generates the expected unpredictable code. If the user sends the same code, the possession of the token is "VERIFIED." With
10 today's powerful computers, it is possible to electronically eavesdrop or otherwise obtain a series of a particular user's codes at different times, and then reverse engineer the algorithm, and unique seed to counterfeit a token.

As mentioned above, however, the preceding approaches must begin with the entity providing the authenticator with the user-identity of the user that the entity purports to be. The
15 security of these approaches can be breached because each requires the communication of the static identifying information. For example, today's powerful computers can be used by an electronic eavesdropper to reverse engineer the algorithm and the seed based on a series of intercepted time-varying codes generated for a particular user. Such an attack would then allow the eavesdropper to counterfeit the user's token.

20 Because of the previously described shortcomings of current approaches, improved identity-authentication is needed to provide sufficient security in view of the processing power of today's computers and the sophistication of today's eavesdroppers.

SUMMARY OF INVENTION

25 According to some embodiments, apparatus, systems and methods employ tokens that never send or transmit any abusable or exploitable static information. For example in one embodiment, an unpredictable number, representing the satisfaction of all three identity factors, is transmitted by radio frequency (RF) to a remote, secure server. In the background, the

- 4 -

remote-server has been generating all non-predictable codes that are being generated on all or a group of authorized tokens. If the transmitted code is matched against the constantly changing database included in the remote server, the user is "IDENTIFIED."

According to various embodiments, identity-authentication is achieved without
5 transmitting any exploitable static information. In one aspect, a system includes a processor configured to generate a non-predictable code using multiple authentication factors for a user in possession of a token. The system includes a secure authentication system (for example, including a database and associated server) that stores multiple authentication factors for a plurality of users, respectively. In one embodiment, the secure system periodically (for
10 example, every minute) generates the non-predictable code associated with each of the plurality of users. When a non-predictable code alone without any static index is transmitted from a user token and received at the secure system, the system operates to compare the received code to all non-predictable codes valid at that time. When a match is found, the user is identified. This approach is in contrast to prior approaches in which the user's identity is
15 "verified."

According to various embodiments, the token includes a mobile phone, a tablet or iPad device or other wireless user-device and the token wirelessly transmits the non-predictable code.

Additional features can be included in combination with the preceding. For example,
20 in some embodiments, a PIN is not stored in the token. Instead, according to this embodiment, the PIN is entered by the user and immediately integrated in an algorithm such that it is not stored, transmitted or otherwise exposed. According to one embodiment, the algorithm includes an exclusive-or operation performed on the PIN. Further, the non-predictable code is generated without being exposed to the user and is transmitted from the token via radio
25 frequency (RF) so that it remains unknown to the user. These approaches increase security, speed and convenience.

For example, according to some embodiments, the generation and transmission of the non-predictable code in the preceding approach avoids constraints on the size of data that is

- 5 -

transmitted from the token because the transmitted value is not manually entered by the user. In addition, the potentially large size of the non-predictable value (for example, 20 digits or more) can exponentially increase security while RF transmission dramatically increases speed and convenience.

5 According to some embodiments, the non-predictable value provides evidence of three factors including something the user is (for example, the biometric), something the user knows (for example, the PIN); and something the user possesses (for example, the token with the associated secret seed). Thus, in one embodiment, successful authentication of identity is only achieved where each of the three factors is valid for generation of a non-predictable value
10 corresponding to the user.

 The robustness of the system can be enhanced in some embodiments by addressing the unlikely circumstance where the same non-predictable code is generated for more than one user for a given time period. According to one embodiment, when the preceding occurs the secure system delays the authentication until the occurrence of immediately subsequent non-
15 predictable code from the next time period to insure that the authentication proceeds based on a unique identification. In some embodiments, the current code and several future codes may be generated at either or both USR and the token for computational efficiency and instant comparisons. According to one embodiment, the codes are generated at USR on a substantially real-time basis.

20 To reduce the risk of a man-in-the-middle attack, embodiments can operate to have the secure system confirm its identity to the token. In one embodiment, the token generates and transmits a first non-predictable code (or portion thereof) to the secure system. This first non-predictable code is not used to execute the authentication used to approve the requested action. Instead, according to this embodiment, the secure system identifies the user based on the first
25 non-predictable code (for example, using a code matching algorithm as described herein) and replies by generating a second non-predictable code (or portion thereof) that corresponds to the code that would be generated by the token during the immediately subsequent time period. The token receives the second non-predictable code and determines whether it is correct by

- 6 -

comparing the code to that which it generates. If so, the remote secure system has proven its identity and the token then generates a third non-predictable value that is transmitted to the secure system where it is employed to authenticate the identity of the user.

According to some embodiments, the systems and methods described herein provide
5 approaches in which the user device (for example, smart phone, tablet, or other form of token) do not store information that can be exploited by a hacker to impersonate the user. In one embodiment, the PIN entered by the user is not authenticated locally at the token. Instead, the PIN is either immediately employed in the generation of a non-predictable value used by a secure registry to authenticate an identity of the user or is transmitted in a protected manner to
10 the secure registry as part of an authentication process, for example, by XORing the PIN with the non-predictable value. Because the PIN is not authenticated locally, the PIN need not be stored by the token. In one embodiment, the user device does not store information that can be exploited by a hacker to impersonate the user.

Unlike prior approaches in which a non-predictable value is encrypted (either in a
15 consistent manner or a varying manner), embodiments described herein do not require encryption of the transmitted non-predictable value because the non-predictable value is transmitted without static identifying information. As a result, an eavesdropper gains no knowledge of the identity of the user even where the eavesdropper intercepts the non-predictable value.

20 In accordance with one aspect, a system for authenticating identities of a plurality of users includes a network having at least a portion that includes a wireless network, a computer coupled to the network, a handheld device configured to communicate with the computer over the wireless network and a secure registry system including a communication interface coupled to the network. In some embodiments, the handheld device includes a user interface
25 programmed to receive user input including secret information known to the user of the handheld device. In addition, the handheld device can include a processor coupled to the user interface where the processor is programmed to authenticate the user of the handheld device and generate a time varying non-predictable value following a successful authentication of the

- 7 -

user by the processor based on the user successfully providing the secret information to the handheld device. Further, the handheld can include a wireless transceiver coupled to the processor and configured to transmit via the network a wireless signal including the time-varying non-predictable value. According to further embodiments, the secure register system includes a communication interface coupled to the network where the secure registry system is configured to receive the time-varying non-predictable value and successfully authenticate the user where the time-varying non-predictable value is matched to the user by the secure registry system. Further, in accordance with some embodiments, a user of the handheld device is permitted to operate the computer to access resources with the computer so long as the computer periodically receives subsequent authentication information that results in a continued successful authentication of the user for time periods subsequent to a time at which the time-varying non-predictable value is generated.

In accordance with some embodiments the handheld device includes a biometric sensor coupled to the processor where the biometric sensor is programmed to receive a biometric input provided by the user and where the processor is programmed to authenticate the user of the handheld device and can generate a time varying non-predictable value following a successful authentication of the user by the processor. In one embodiment, the biometric sensor includes a microphone configured to receive a spoken input provided by the user and the user interface is programmed to display a multicharacter string including at least one of a plurality of alpha-characters and a plurality of numeric-characters, and further where the processor is programmed to authenticate the user based on the spoken input of the multicharacter string by the user. In accordance with some embodiments, the secure registry system is programmed to randomly generate the multicharacter string and communicate the multicharacter string by the network to the handheld device for display.

In accordance with another aspect, a method of authenticating identity using a secure registry system is provided where the secure registry system includes a processor, a communication interface coupled to the processor and database coupled to the processor where the database is configured to store seed for each of the plurality of user respectively and the

- 8 -

processor is configured to generate time-varying non-predictable values using the respective seeds. In accordance with some embodiments, the method includes receiving at the secure registry system a first time-varying non-predictable value generated by a first handheld device in possession of the user the first time-varying non-predictable value generated using a seed
5 associated with the first handheld device and a first time. Further, the method can include identifying, by the secure registry, the user based on the first time-varying non-predictable value and generating a second time-varying non-predictable value with the secure registry. In one embodiment, the second time-varying non-predictable value is generated using the seed associated with the first handheld device and a second time where the second time is
10 subsequent to the first time.

In addition, in accordance with some embodiments, the method may also include communicating at least a portion of the second time-varying non-predictable value to the first handheld device. In these embodiments, the second time-varying non-predictable value is employed by the first handheld device to communicate the identity of the secure registry
15 system by confirming that the second time-varying non-predictable value is valid when generated using the seed at the second time. Further, the method may include authenticating an identity of the user by the secure registry system using the third time-varying non-predictable value generated by the first handheld device and received by the secure registry system. In accordance with these embodiments, the third time-varying non-predictable value is
20 generated using the seed associated with the first handheld device and a third time subsequent to the second time.

In some embodiments, a method of securing a computing device can include receiving at the computing device a first wireless signal including first authentication information wirelessly transmitted from a mobile device proximate to the computing device, processing,
25 the first authentication information to initially authenticate a user in possession of the mobile device, the user, attempting to access resources with a computing device. The method can also include temporarily allowing the user to employ the computing device to access the resources when the initial authentication is successful and continuing to allow the user to employ the

- 9 -

computing device to access the resources upon a continued receipt of authentication information from a mobile device that is successfully authenticated. Still further, the method can include automatically terminating use of the computing device by the user based on at least one of: authentication information no longer being received from the mobile device and
5 authentication information received from mobile device no longer being successfully authenticated.

BRIEF DESCRIPTION OF DRAWINGS

The accompanying drawings are not intended to be drawn to scale. In the drawings,
10 each identical or nearly identical component that is illustrated in various figures is represented by a like numeral. For purposes of clarity, not every component may be labeled in every drawing. In the drawings:

FIG. 1 is a functional block diagram of a computer system configured to implement the universal secure registry (“USR”), including a USR database, according to one embodiment of
15 the invention;

FIG. 2 is a functional block diagram of a first embodiment of a networked environment including the computer system of FIG. 1;

FIG. 3 is a functional block diagram of an entry of a database forming the USR database of FIG. 1 in accordance with one embodiment;

20 FIG. 4 is a flow chart in accordance with one embodiment;

FIG. 5 is a flow chart in accordance with another embodiment;

FIG. 6 is a flow chart in accordance with still another embodiment;

FIG. 7 is a functional block diagram of a system in accordance with some
embodiments;

25 FIG. 8 is a functional block diagram of a system in accordance with some further
embodiments;

FIG. 9 is a flow chart in accordance with one embodiment;

FIG. 10 is a flow chart in accordance with one embodiment;

- 10 -

FIG. 11 is a system block diagram in accordance with one embodiment; and
FIG. 12 is a system block diagram in accordance with one embodiment.

DETAILED DESCRIPTION

5 This invention is not limited in its application to the details of construction and the arrangement of components set forth in the following description or illustrated in the drawings. The invention is capable of other embodiments and of being practiced or of being carried out in various ways. Also, the phraseology and terminology used herein is for the purpose of description and should not be regarded as limiting. The use of “including,” “comprising,”
10 “having,” “containing,” “involving,” and variations thereof herein is meant to encompass the items listed thereafter and equivalents thereof as well as additional items.

 As used herein, “USR” generally refers to a secure registry, for example, a remote secure registry. In some embodiments, USR is employed as a secure, central repository for a variety of confidential personal information. In various embodiments, this personal
15 information can be used to authenticate an identity in support of any of the following activities: Credit/Debit Card Purchases; Check Purchases; Wiring Funds; Accessing bank and other financial records; transferring funds between individuals; transferring funds between an individual and vendor and vending machine; providing a form of identification; unlocking and starting a vehicle; unlocking and entering a home, office, hotel room or other secure physical
20 space; accessing secure physical facilities such as a military base or nuclear reactor; completing applications for loans, mortgages, credit or jobs; accessing and/or logging into a computer, a computer network or a secure server; and completing medical (or other types of) forms.

 In some embodiments, an information system is formed as a computer program running
25 on a computer or group of computers configured to provide a universal secure registry (USR) system. The computer, in this instance, may be configured to run autonomously (without the intervention of a human operator), or may require intervention or approval for all, a selected subset, or particular classes of transactions. The invention is not limited to the disclosed

- 11 -

embodiments, and may take on many different forms depending on the particular requirements of the information system, the type of information being exchanged, and the type of computer equipment employed. An information system according to this invention, may optionally, but need not necessarily, perform functions additional to those described herein, and the invention
5 is not limited to a computer system performing solely the described functions.

In the embodiment shown in FIG. 1, a computer system 10 for implementing a USR system according to the invention includes at least one main unit 12 connected to a wide area network, such as the Internet, via a communications port 14. The main unit 12 may include one or more processors (CPU 16) running USR software 18 configured to implement the USR
10 system functionality discussed in greater detail below. The CPU 16 may be connected to a memory system including one or more memory devices, such as a random access memory system RAM 20, a read only memory system ROM 22, and one or more databases 24. In the illustrated embodiment, the database 24 contains a universal secure registry database. The invention is not limited to this particular manner of storing the USR database. Rather, the USR
15 database may be included in any aspect of the memory system, such as in RAM 20, ROM 22 or disc, and may also be separately stored on one or more dedicated data servers. According to some embodiments, cloud computing is employed such that access to the USR and associated features and elements is remotely available to users and/or administrators.

The computer system may be a general purpose computer system which is
20 programmable using a computer programming language, such as C, C++, Java, or other language, such as a scripting language or even assembly language. The computer system may also be specially programmed, special purpose hardware, an application specific integrated circuit (ASIC) or a hybrid system including both special purpose components and programmed general purpose components.

25 In a general purpose computer system, the processor is typically a commercially available microprocessor, such as Pentium series processor available from Intel, or other similar commercially available device. Such a microprocessor executes a program called an operating system, such as UNIX, Linux, Windows NT, Windows 95, 98, or 2000, or any other

- 12 -

commercially available operating system, which controls the execution of other computer programs and provides scheduling, debugging, input/output control, accounting, compilation, storage assignment, data management, memory management, communication control and related services, and many other functions. The processor and operating system defines a
5 computer platform for which application programs in high-level programming languages are written.

The database 24 may be any kind of database, including a relational database, object-oriented database, unstructured database, or other database. Example relational databases include Oracle 8i from Oracle Corporation of Redwood City, California; Informix Dynamic
10 Server from Informix Software, Inc. of Menlo Park, California; DB2 from International Business Machines of Armonk, New York; and Access from Microsoft Corporation of Redmond, Washington. An example object-oriented database is ObjectStore from Object Design of Burlington, Massachusetts. An example of an unstructured database is Notes from the Lotus Corporation, of Cambridge, Massachusetts. A database also may be constructed
15 using a flat file system, for example by using files with character-delimited fields, such as in early versions of dBASE, now known as Visual dBASE from Inprise Corp. of Scotts Valley, California, formerly Borland International Corp.

The main unit 12 may optionally include or be connected to an user interface 26 containing, for example, one or more input and output devices to enable an operator to
20 interface with the USR system 10. Illustrative input devices include a keyboard, keypad, track ball, mouse, pen and tablet, communication device, and data input devices such as voice and other audio and video capture devices. Illustrative output devices include cathode ray tube (CRT) displays, liquid crystal displays (LCD) and other video output devices, printers, communication devices such as modems, storage devices such as a disk or tape, and audio or
25 video output devices. Optionally, the user interface 26 may be omitted, in which case the operator may communicate with the USR system 10 in a networked fashion via the communication port 14. It should be understood that the invention is not limited to any particular manner of interfacing an operator with the USR system.

- 13 -

It also should be understood that the invention is not limited to a particular computer platform, particular processor, or particular high-level programming language. Additionally, the computer system may be a multiprocessor computer system or may include multiple computers connected over a computer network. It further should be understood that each
5 module or step shown in the accompanying figures and the substeps or subparts shown in the remaining figures may correspond to separate modules of a computer program, or may be separate computer programs. Such modules may be operable on separate computers. The data produced by these components may be stored in a memory system or transmitted between computer systems.

10 Such a system may be implemented in software, hardware, or firmware, or any combination thereof. The various elements of the information system disclosed herein, either individually or in combination, may be implemented as a computer program product, such as
15 USR software 18, tangibly embodied in a machine-readable storage device for execution by the computer processor 16. Various steps of the process may be performed by the computer processor 16 executing the program 18 tangibly embodied on a computer-readable medium to perform functions by operating on input and generating output. Computer programming languages suitable for implementing such a system include procedural programming languages, object-oriented programming languages, and combinations of the two.

As shown in FIG. 2, the computer system 10 may be connected to a plurality of
20 interface centers 27 over a wide area network 28. The wide area network 28 may be formed from a plurality of dedicated connections between the interface centers 27 and the computer system 10, or may take place, in whole or in part, over a public network such as the Internet. Communication between the interface centers 27 and the computer system 10 may take place according to any protocol, such as TCP/IP, ftp, OFX, or XML, and may include any desired
25 level of interaction between the interface centers 27 and the computer system 10. To enhance security, especially where communication takes place over a publicly accessible network such as the Internet, communications facilitating or relating to transmission of data from/to the USR

- 14 -

database 24 or the computer system 10 may be encrypted using an encryption algorithm, such as PGP, DES, or other conventional symmetric or asymmetric encryption algorithm.

In one embodiment, the USR system 10 or USR database 24 may be able to authenticate its identity to a user or other entity accessing the system by providing an appropriate code which may be displayed on the user's smart card, mobile device such as a mobile phone, ipad, tablet, laptop, netbook, or on a desktop computer as some examples. A comparison by the user or the code generator between the provided number and an expected number can validate, to the user (or other entity) or a code generator included in the user-device, that communication is with the database and not an imposter. In another embodiment, a challenge-response protocol is employed to authenticate the identity of the USR system and/or the user to the other.

The database 24 shown in FIG. 1 has a USR database containing entries related to persons 1-n. The data in the USR database may also be segregated, according to data type to enable individual computer modules to handle discrete applications on discrete data types. Segregating the data in modules may make access to the database more robust by enabling portions of the data in the USR database 24 to be accessible even when it is necessary to perform maintenance on a portion of the database. However, storing the data in the USR database 24 according to the scheme illustrated in FIG. 1 may make it easier for a user of the database to make changes to multiple types of data simultaneously or in a single session. There are advantages and disadvantages to each data structure, and the invention is not limited to a particular manner of organizing the data within the database 24, data structures other than the two shown also being possible.

As shown in FIG. 3, each entry 30 in the database 24 may contain multiple types of information. For example, in the embodiment shown in FIG. 3, the entry contains authentication information 32, access information 34, publicly available information 36, address information 38, credit card and other financial information 40, medical information 42, job application information 44, and tax information 46. The invention is not limited to a USR containing entries with all of this information or only this particular information, as any

- 15 -

information on a person or other entity such as a company, institution, etc. may be stored in
USR database 24.

If the database information is split between multiple databases, each database will
typically include at least the authentication and access information to enable the USR software
5 to correlate an authentication attempt with a valid authentication, and to enable the USR
software to determine access privileges to the requested data. Alternatively, databases may be
linked to permit information not in a main USR database to be retrieved, with successful
authentication for all databases accessed being done at the USR system.

In FIG. 3, the authentication information is information about the user of the database
10 to whom the data pertains and is to be used by the USR software 18 to validate that the person
attempting to access the information is the person to whom the data pertains or is otherwise
authorized to receive it. The authentication information may be any type of information that
will reliably authenticate the identity of the individual. For example, in some embodiments,
the information may include any of a secret known by the user (e.g., a pin, a phrase, a
15 password, etc.), a token possessed by the user that is difficult to counterfeit (e.g., a secure
discrete microchip), and/or a biometric information concerning a biometric, for example, a
voiceprint, a fingerprint, DNA, a retinal image, a photograph, etc.

The user's authentication information may be manually entered or scanned at the
interface center. However, a variety of types of communication may be employed to
20 communicate the user's identifying information from the user-device to the computer system.
For example, near field signal may be employed to communicate information between the
user-device and the computer system 10. According to one embodiment, the user's
authentication information is included in (or entered via) the user's cell phone where it is then
communicated to the computer system 10. In one embodiment, the cell phone is also
25 configured to receive information from the computer system 10 at the interface center 27.

In one embodiment, the user of the database will carry a user-device that allows for
secure access to the USR database without requiring the user to transmit any personal
information. In one embodiment, to access the USR database, the user-device retrieves a

- 16 -

secret seed associated with the device and/or time varying value from memory and obtains from the user a secret personal identification code. The user-device mathematically combines these three numbers using a predetermined algorithm to generate a one-time non-predictable code which is transmitted to the computer system 10. The computer system, specifically USR
5 software 18, utilizes the received one-time non-predictable code to determine whether the user is authorized access the USR database and grants access to the USR database if the user is determined to be authorized. The authentication information 32 in the database entry in the embodiment of the invention illustrated in FIG. 3 contains information to enable the USR software 18 to validate the user using such a card in this manner.

10 Alternative types of identification cards or tokens may likewise be used. For example, other smart cards may be used which generate non-predictable single use codes, which may or may not be time varying, or other access code generators may be used. An algorithm generating such non-predictable codes may also be programmed onto a processor on user-devices such as smart cards or other computing devices, such as a cell phone, pager, ID badge,
15 wrist watch, computer (for example, desktop, laptop, netbook, tablet), personal digital assistant, key fob, or other commonly available electronic device. For convenience, the term "electronic ID device" will be used generically to refer to any type of electronic device that may be used to obtain access to the USR database.

Likewise, various types of biometric information may be stored in the authentication
20 area of the database entry to enable the identity of the user possessing the identifying device to be authenticated at the point of use. Examples of the type of biometric information that may be used in this situation includes a personal identification number (PIN), fingerprint, voice print, signature, iris or facial scan, or DNA analysis. If desired, the verifying section of the database may contain a picture to be transmitted back to the person seeking to validate the device to
25 ensure the person using the device is the correct person. Optionally, the identifying device itself may also be provided with a picture of the person authorized to use the card to provide a facial confirmation of the person's right to use the card.

- 17 -

Further, a challenge-response protocol may be employed in combination with or as an alternative to the preceding to validate the person attempting to access the information. Various embodiments may employ a challenge-response protocol with or without an identification card.

5 In FIG. 3, the Access information 34 is provided to enable different levels of security to attach to different types of information stored in the entry 30 in the USR database 14. For example, the person may desire that their address information be made available only to certain classes of people, for example colleagues, friends, family, Federal Express, U.P.S., and the U.S. mail service. The names or universal identifiers for those selected individuals,
10 companies, organizations and/or agencies may be entered into appropriate fields in the Access information to specify to the USR software 18 those individuals to whom the address information may be released. Likewise, access fields may be specified for the other types of information. For example, the individual may specify that only particular individuals and/or
15 companies have access to the credit card and other financial information 40, medical information 42, job application information 44 and tax information 46. Additionally, the individual may specify that no one have access to that information unless the individual participates in the transaction (see FIG. 6).

As shown in FIG. 1, the USR software 18 contains algorithms for execution by the CPU 16 that enables the CPU 16 to perform the methods and functions of the USR software
20 described herein. The USR software 18, in this embodiment, performs all functions associated with validating an electronic ID card. If desired, a separate authentication software module may be provided to validate electronic ID devices outside of a firewall segregating the authentication information from other user information.

This algorithm comprising the USR software 18 may be used to implement, in one
25 exemplary embodiment, a USR system configured to enable selected information to be disseminated to selected individuals in a secure and dynamic fashion. This information may be used for numerous purposes, several of which are set forth below and discussed in greater detail below.

- 18 -

For example, the USR system may be used to identify the person, enable the person to be contacted by telephone or mail anonymously, enable the person to be contacted by telephone or by mail without revealing the person's telephone number or present location, enable the person to purchase items over the Internet or in a store without revealing to the merchant any personal identification information or credit card information, enable the person to complete a job application without completing a job application form, enable the police to discern the person's identity and any outstanding warrants on the individual, and numerous other uses. The invention is not limited to these several enumerated uses, but rather extends to any use of the USR database.

FIG. 4 illustrates a flow chart of a process 420 for identification of an entity employing the USR. In the illustrated embodiment, the process 420 begins at act 422 where a user registers with the USR. In various embodiments, the registration process can be accomplished remotely over any one of or any combination of wide area networks, local area networks including GSM, Bluetooth, near field communication and Wi-Fi, as some examples. The registration process can include the communication of the user's image, for example, a digital photograph of the user's face that is stored at the USR for use in authenticating the identity of the user in various situations. Further, in various embodiments, the process can require that the user's image be periodically updated to make sure that the image remains current. Other biometric information can also be provided by the user during the registration process, for example, the user can speak the numbers 0-9 for later use in activation of a mobile device as described further herein. This information can be stored with the authentication information as illustrated in FIG. 3.

At act 424, an application, for example, a software application is communicated from the USR to the user's mobile device when the registration is complete. The application can include any of a variety of software programs configured to operate on the user's mobile device, for example, applications programmed for, or using, any of the Java® Platform, Micro Edition (ME), the Android® platform, Linux®, .NET Compact Framework, BREW (Binary Runtime Environment for Wireless), the Symbian platform, the Qt framework, Windows

- 19 -

Mobile®, Palm® OS, as well as applications developed for proprietary operating systems such as Blackberry® by Research In Motion of Waterloo, Ontario, Canada, and iOS by Apple Inc. of Cupertino, Calif.

At act 426, a digital seed which may be encrypted is communicated from the USR to the user's mobile device. In general, the seed is employed to generate a random number, for example, a time varying random number that can be used to identify the user. In some embodiments, the seed is combined with an electronic serial number (ESN) of the token and a digital representation of the time interval. Thus, in accordance with some embodiments, the seed itself is generated in a random fashion at the USR and then stored such that it is associated with the user and can later be used to derive random or pseudo-random one-time codes that are generated at the user device and also at the USR, as is explained further herein.

In accordance with some embodiments, the seed is generated in a random, relatively non-deterministic fashion by the USR using one or a combination of the following non-limiting examples: a real time clock; a counter included in the USR that measures an unstable property of an element (for example, the settling time of an unstable phased locked loop circuit) or the characteristics of a random external event; an analog signal (for example, a voltage produced by noise or data) which is generated by or received by the USR; a random number generator or cryptofunction included in the USR (for example, a multi-stage random number generator; an xorshift random number generator; a linear congruential generator algorithm), the elapsed time of an external function (for example, a wireless message transfer time), or a random number generator provided by an application programming interface (API) included in the USR.

Communication of the seed can be completed over any of a wide area network or a local area network or a combination of both wide area networks and local area networks. For example, the seed can be communicated through a cellular network to a mobile device such as a smart phone. In accordance with other embodiments, the seed can be communicated to the mobile device via a wide area network such as the Internet to a user's personal computer from which it can be communicated to the mobile device via a hardwire USB connection or any

- 20 -

manner of wireless connections such as Bluetooth communication. According to one embodiment, the seed is communicated to the mobile device along with the application. In addition, the seed can thereafter be updated as described below.

5 In accordance with some embodiments, for example, where USR is employed in a system for proximity-based computer security using a wireless user-device (for example, as described in association with FIG. 12) the computer can have a USR element that includes a seed associated with each user authorized to unlock the computer to access resources. In these embodiments, updates to the seed or seeds included in the USR element at the computers can be updated as described above to maintain current information in the computer for the user(s).

10 At act 428, the user requests authorization from the USR for any of a secure payment, authorization for other types of financial transactions, authorization for access to a secure network or physical space, or authorization for any of the activities described previously for which the USR can be employed to authorize the user's action to a third party. That is, once the mobile device is provided with the application and the seed is communicated to the mobile
15 device, the user has the elements in place with which they can employ the process 420 as generally shown in FIG. 4 to identify themselves in a secure manner to a USR. Accordingly, in some embodiments, the process 420 ends at act 426 for user registration and system activation. Thereafter, the process 420 later begins at act 428, when the user requests authorization to take one or a plurality of the listed actions.

20 Beginning at act 430, the process 420 illustrates a general approach employing the USR to identify the user to authorize an action requested by the user either directly by the user or via an intermediary, for example, a third party conducting a transaction with the user. At act 430, the user employs the mobile device to generate a one-time code, for example, a one-time non-predictable pseudo random code. According to one embodiment, the random code is generated
25 by employing a combination of time and the seed that was previously assigned to the user and communicated to the mobile device. In some embodiments, the ESN is employed with the preceding. As described further herein, embodiments can allow the time to be substantially synchronized between the USR and the mobile device to provide a highly secure manner of

- 21 -

identifying the user. Further, the seed that is assigned by the USR is stored and maintained by the USR such that the USR has all the information required by which it can generate the random one-time code that corresponds to the random one-time code generated using the mobile device.

5 In accordance to some embodiments, the USR maintains a database for a plurality of user's where the database includes a random seed that is unique to each user where the seeds are assigned by the USR server. As used herein, the term unique indicates that there is no probability that the USR will assign an identical seed (that is, a seed having an identical value) to more than one user for example, pseudo-random seed generation with the result compared to
10 all previously generated seeds and rejected if there is a match.

 According to various embodiments, the random one-time code is a discrete value that is generated by an algorithm that employs a combination of the seed assigned to the user via the USR and at least one of time (for example, Coordinated Universal Time), an electronic serial number of the mobile device, a SIM card number of the SIM card included in the device and a
15 PIN number provided by the user. According to some embodiments, any of the seed, the electronic serial number, the SIM card number and the PIN can be stored in a secure element provided with the mobile device. In various embodiments, the secure element can include a microcontroller, memory or other electronic components that can be provided in the mobile device. Further, in various embodiments, the random one-time code is generated by
20 employing a PIN in combination with any one of or any combination of an electronic serial number of the user-device, a SIM number of the user-device and a seed associated with the device.

 In accordance with one embodiment, at act 434, the USR employs a code-matching algorithm to locate a match between the random one-time code communicated from the mobile
25 device and the random one-time codes that are calculated for each of a plurality of registered users as provided by the USR. That is, because the USR can host tens of millions or more registered users, the USR is programmed to conduct code-matching searches by first determining a current code associated with each user and then comparing the random one-time

- 22 -

code received from the user by the mobile device with all the codes calculated for that moment in-time by the USR. At act 436, the user is identified if a match is found. The USR then reviews the authorization request to determine whether the identified-user has the permission required to take the requested action, i.e., the USR determines whether the requested action is
5 consistent with those associated with the user.

According to some embodiments, registered users are organized into groups, for example, based on the geography, to reduce the plurality of users that are processed with the code-matching algorithm on receipt of a random one-time code. In one embodiment, location information can be transmitted with the random one-time code from a user's mobile device.

10 According to some embodiments, the approach illustrated in FIG. 4 can be employed over periods of time for a variety of authorized activities requested by the user. Thus, at act 438, the mobile device and the USR are available for identification to support the user's subsequent activities as needed. In accordance with the illustrated embodiment, the process begins again for a subsequent act at act 426, however, in some embodiments, the process can
15 begin at act 428. Where, for example, the same seed is to be employed in the subsequent authorization request made relatively close in time to the first request.

FIG. 4 also illustrates an embodiment in which there are a plurality of ongoing actions that can take place in the process 420. For example, at act 440, an updated seed is assigned to the user by the USR and communicated to the mobile device. The preceding can be conducted
20 at a known interval (i.e., periodically) or in a more random nature that is sufficient to maintain the level of security required of the process 420. Thus, in various embodiments, the updated seed can be provided at act 440 on the frequency of less than one minute, between one and fifteen minutes, hourly, daily, weekly, or at some other interval that is either a known frequency or a variable frequency. In some embodiments, the interval can be established to
25 achieve a desired level of security, for example, where the more frequently the seed is updated the greater the security.

As also illustrated in FIG. 4, according to some embodiments, the process 420 can be used to assist a user in making payments and/or fund transfers from the user's account which is

- 23 -

maintained with the USR. As is described in greater detail herein, such an approach can provide the user with a means by which the mobile device can be employed to transfer funds between their account and the account of another authorized user after the parties have agreed to the transfer and after the USR has been employed to identify the parties to the transaction.

5 In addition, the USR can be employed to maintain the accounts such that the transfer of funds occurs within the USR from an account of a USR-account of the payer to a USR-account of the payee.

According to one embodiment, the user can establish a fund's transfer account with the USR during the act of registration 422 or sometime thereafter. In the illustrated embodiment, 10 the user establishes the funds-transfer account at Act 442. Further, the user can activate the account by transferring funds to the USR, for example, such as electronically transferring the funds, wiring the funds, charging the funds to an account or mailing a check to the USR administrators. Once populated with funds, the account can be employed to make or receive payments or otherwise transfer funds between their accounts and the accounts of other 15 authorized, registered USR users.

In some embodiments, authorized users (that is, payors or payees) are established on temporary, real-time basis to conduct a one-time transaction. In further embodiments, registered USR users are authorized by a payor for an anticipated series of transactions over a longer period of time in the future.

20 Further, one of the ongoing actions illustrated in 420 includes the act 444 at which automatic replenishment of funds can be applied to the user's account. Such an approach can rely on preauthorized transfers or debits from the user's existing bank accounts or other forms of electronic transfer funds such as a transfer of funds from a credit card or debit account. The acts 442 and 444 are illustrated in phantom because they are optional in accordance with some 25 embodiments.

Referring now to FIG. 5, a process 460 is illustrated by which a user can employ a mobile device to receive an authorization for one or more of the user's activities. Some embodiments include a process by which a user activates a mobile device for use in having

- 24 -

their identification confirmed. According to one embodiment, the process 460 includes act 462 in which a user enters a PIN number in their mobile device and at Act 464, the PIN number is communicated to the USR, for example, in an encrypted form. According to some embodiments, at Act 466, the USR compares the PIN to PINs associated with a plurality of users all stored at the USR, and where the PIN matches the identity of a user, communicates the multi-character numeric value to the user's mobile device. According to this embodiment, the user's spoken input of the numeric value is employed to authenticate the user to activate the mobile device for use in an identification process with the USR. Thus, in accordance with one embodiment, the user's spoken input is communicated to the USR for authentication in order to activate the mobile device. According to another embodiment, at Act 466, the authentication of the user's spoken input is accomplished at the mobile device. In other embodiments, the mobile device can have limited functionality (for example, allowing a user to make phone calls or browse the Internet) prior to device activation while preventing the mobile device from being employed to execute secure transactions or take other actions that require interaction with USR based-authentication until a device activation process is complete (for example, acts 462, 464 and 466 of the process 460).

In some embodiments, entry of a PIN is not required. Instead, a selection of the USR application results in the multi-character value being presented to the user in a display of their mobile device. The user's spoken input of the multi-character value is then authenticated at act 466.

According to various embodiments, the device activation portion of the process 460 (the acts 462, 464, and 466) can differ from that described above, for example, the PIN may be used to derive a non-predictable value that is used to identify the user prior to communication of the multi-character numeric value. In still further embodiments, the process 460 does not include the acts 462, 464 and 466.

Although the process 460 is described as employing a multi-character numeric value, other embodiments can employ a multi-character string that includes either or both alpha or numeric characters. In some embodiments, the user interface of the mobile device (for

- 25 -

example, the wireless user device 652, 735) is configured to display a multi-character string including at least one of a plurality of alpha-characters and a plurality of numeric-characters where a processor included in the mobile device is programmed to authenticate the user based on the spoken input of the multi-character string by the user. In a further embodiment, the processor included in the mobile device is programmed to authenticate the spoken input on a character-by-character basis.

According to various embodiments, the device activation portion of the process 460 (the acts 462, 464, and 466) can be employed by a user to allow their identity to be confirmed and their actions authorized in any of a wide variety of environments and situations. For example, at act 468, the activated mobile device can be employed with the mobile device to make a financial payment or credit/debit card payment or funds transfer using the USR. At act 470, the mobile device can be activated to make a direct personal payment and/or funds transfer between accounts within the USR, including third-party accounts. In accordance with a further embodiment, at act 472, the device can be activated to allow the user's identity to be determined and their actions authorized in a number of other situations, for example, to gain access to a secure computer network, to perform other types of commercial transactions, to proceed through security checkpoints, access physical facilities, etc.

Returning again to act 468 and the use of the mobile device with USR based identification system, the process 460 can be employed at a point-of-sale. For example, a user located in a store or other commercial environment at the point-of-sale. The transaction details are communicated from the point-of-sale to the mobile device for review by the user. Such transaction details can include information, for example, the purchase amount, the name of the vendor, time and date, and even a list of the individual item or items that are being purchased. This provides the user with an opportunity to review and approve the transaction on their mobile device. At act 474, the user can elect to accept the transaction by, for example, selecting an element in the user interface of the mobile device or cancel the transaction. Where, for example, the user elects to cancel the transaction, the process 460 ends at act 476. Alternatively, should the user accept the transaction, the process moves to act 478. At act 478,

- 26 -

the mobile device generates a random one-time code as described, for example, in the embodiments of FIG. 4. At act 480, the one-time code is communicated to the USR along with the transactions details. In some embodiments, the transaction details can include a code representing one of a plurality of accounts.

5 The communication with the USR can occur via the POS or independent of the POS, depending on the embodiment. At act 482, the USR receives the random one-time code and employs the code-matching search to identify the user. The user is identified when a match is found between the random one-time code communicated to the USR and the USR-calculated codes determined for the registered group or groups of users. This registered group or groups
10 of users can be those other registered users who also employ the identification approach described herein. Alternatively, the various group or groups can be divided into subgroups of users who may have some common association or identifying feature that USR can employ in organizing and segmenting the data in the database to increase the processing speed of the code-matching algorithm. Regardless of the size of the group, however, the USR employs a
15 code-matching search and identifies the user when a match is found between a USR-calculated code included among a plurality of codes calculated for the plurality of users, respectively, and the code generated with the mobile device.

At act 484, the USR determines whether the identified-user is authorized to complete the transaction, for example, does the identified-user have a financial account with USR and if
20 so are they credit-worthy. At act 488, the USR communicates a denial of a transaction if the identified user is not authorized to complete such a transaction. At act 486, the USR communicates an authorization, for example, communicates the authorization to the point-of-sale along with a digital image of the user if the identified user is authorized to complete the transaction. The digital image may come directly from USR or partially from USR and
25 partially from the mobile device.

According to some embodiments, the random one-time code generated at act 478 is communicated along with static identifying information at act 480, for example, where a verification process is employed to authenticate the identity of the user of the mobile device.

- 27 -

According to other embodiments, static identifying information is not communicated to USR with the random one-time code generated at act 478, for example, where an identification process is employed to authenticate the identity of the user of the mobile device.

5 In addition, a device activation process (for example, the device activation provided in by acts 462, 464, 466) can be employed without the remaining acts included in the process 460 illustrated in FIG. 5. For example, the acts 462, 464, 466 can be employed independently in a process that may not include any communication with the USR and/or may not include generation of a one-time code using the mobile device.

Referring now to FIG. 7, a functional block diagram of the USR is illustrated in
10 accordance with one embodiment. According to some embodiments, the USR 640 is employed to identify a user from among a plurality of users based on the receipt of a random one-time code from a remote system element. According to various embodiments, the remote system element can include any of: an electronic device such as a handheld electronic device; a point-of-sale device; a computer, server or other network device, for example, wireless user
15 devices 652 and 735 described herein. Accordingly, in some embodiments the remote system element includes a mobile phone such as a smart phone. Further, in some embodiments, any of the elements illustrated in FIG. 7 can be included in the USR systems or portions thereof illustrated in FIGS. 1-3 either alone or in any combination with other elements described herein.

20 In the embodiment illustrated in FIG. 7, the USR 640 includes a seed generation module 642, a database of assigned seeds 644, a generation module 646, a time reference 648, a comparison module 645, a first communication module 647 and a second communication module 649. Other arrangements and system configurations are possible depending upon the desired functionality. For example, the embodiment illustrated in FIG. 7 can be employed with
25 the USR system configurations illustrated herein. Accordingly, in some embodiments system elements that communicate with the USR to execute the processes illustrated in Figs. 32, 33 and 34 can include any of the mobile device 674, the POS terminal 676, the interface device 682, the mobile device 652, the network access device 658, the wireless user-device 735 and

- 28 -

the computer 736 as some examples. In some embodiments, one or more of the preceding system elements can communicate with the system 640 via the second communication module 649. Further, functionality other than that illustrated in FIG. 7 can also be provided with the USR. In particular, the USR illustrated in FIG. 7 can include functionality such as any or
5 select portions of the functionality described herein concerning other embodiments of the USR. Further, any of the illustrated modules can be configured in hardware, software or a combination of hardware and software depending upon the embodiment.

Accordingly, it should be appreciated that embodiments can include other modules and/or modules configured differently than those illustrated. For example, the first
10 communication module 647 and the second communication module 649 can be included in the same module; the comparison module 645 can include a database, data-table or data-tree to store the current random one-time codes for comparison, or alternatively, a separate database, data-table or data-tree can be included to store the current random one-time codes which are provided to the comparison module 645 for comparison. In various embodiment s, each of the
15 modules included in the USR 640 is coupled to others of the modules.

According to one embodiment, the seed generation module 642 is in communication with at least the database module 644 and the second communication module 649. The database module 644 is in communication with at least with the generation module 646. Further, in the illustrated embodiment, the time reference 648 is in communication with the
20 generation module 646. In addition, the generation module 646 is in communication with the comparison module 645, while the comparison module 645 is also in communication with each of the first communication module 647 and the second communication module 649.

In accordance with one embodiment, the seed generation module 642 operates to randomly generate (for example, without replacement) and assign seeds for a plurality of users
25 registered with the USR, for example, users 1-N. Further, the generation module 642 communicates the seeds and their assignments to the database module 644 where the assigned seed associated with each user for a given time period are stored in association with one another such that they can be searched and retrieved. According to a further embodiment, a

- 29 -

separate assignment module is included in the USR and operates to receive the seeds from the seed generation module 642 and assign the seeds to the plurality of users. In accordance with various embodiments, the database module 644 can include a relational database such as relational database such as Oracle® Database by Oracle Corp. of Redwood Shores, Calif.,
5 Advantage Database Server or SQL Anywhere, each by Sybase of Dublin, Calif., MySQL™ by Sun Microsystems of Santa Clara, Calif., DB2® by IBM Corp. of Armonk, N.Y., or InterBase by Embarcadero Technologies of San Francisco, Calif. In other embodiments, the database module can include an object-oriented database such as InterSystems CACHÉ by InterSystems Corp. of Cambridge, Mass., JADE by Jade Software Corp. of Christchurch, New
10 Zealand, or FastObjects by Versant Corp. of Redwood City, Calif.

In accordance with some embodiments, the second communication module 649, communicates seeds to the system elements including user-devices, secured computers and other elements included in the USR system. In one embodiment, seed updates are performed without requiring any user interaction. For example, in one embodiment, a seed in a user
15 device or remote USR element (for example, the USR element 768 illustrated in FIG. 12) is updated in the background at a time when the device or registry element are in communication. In a further embodiment, the update occurs without knowledge of the user. Thus, the systems described herein can include automatic reseeding of remote end user devices and USR systems elements.

20 In accordance with the illustrated embodiment, the generation module 646 receives a time reference from the time reference module 648 and receives the assigned seeds and users from which it generates random one-time code at the time T for the users 1-N and communicates that information to the comparison module 645.

25 According to some embodiments, the comparison module 645 receives, via communication module 647, a random one-time code from a remote system element such as mobile device, POS device or the like and compares, using a code-matching search, the received random one-time code with those generated by the generation module 646 to determine whether a match exists. Depending on the embodiment, the communication of the

- 30 -

random one-time code can be over a network such as the networks 28, 656 and 738 as illustrated and described herein. According to some embodiments, the current codes of a plurality of users are organized in a table, for example, a table that is organized numerically. In one embodiment, the table can be searched using a search algorithm such as a binary search.

5 In a further embodiment, the search begins by comparing the value that is sought to the middle item of the table. If the value matches the middle item, the search is successful. If the value is less than the middle item, then the higher half of the table is eliminated from the search. If the value is greater than the middle item, then the lower half of the table is eliminated. The process is then repeated, for example, depending on the embodiment either iteratively or

10 recursively, within each remaining half of the table until a match is identified. According to various embodiments, other search techniques may be used to search the table.

In other embodiments, the current codes of the plurality of users are organized in a tree data structure. According to one embodiment, the tree can be searched using a search algorithm, such as a binary search tree. For example, a tree can include a plurality of nodes

15 connected in a hierarchical tree structure, where each node to the left of a root node only contains a value less than the value that is contained in the root node, and where each node to the right of the root node only contains a value greater than contained in the root node. Using a binary search tree, the search begins by comparing the value that is sought to a value stored in the root node of the tree. If the value matches, the search is successful. If the value is less than

20 the value of the root node, for example, then the nodes of the left subtree are searched iteratively or recursively. If the value is greater than the value of the root node, then the nodes of the right subtree are searched. This process is repeated, descending the nodes of each subtree, until a match is identified. According to various embodiments, other search techniques may be used to search the tree data structure.

25 As should be appreciated, the USR 640 illustrated in FIG. 7 can be employed in embodiments that use an identification process and embodiments that use a verification process. Where an identification process is used, the random one-time codes received by the first communication module 647 are received without any static identifying information. The

- 31 -

comparison module 645 compares the received code with the current codes for a plurality of users to authenticate an identity of the user. Where a verification process is employed, a static nominal constant is included with the random one-time code, for example, appended to the random one-time code as a suffix or prefix. Here, the comparison module 645 indexes the
5 database by the static number to verify an identity of the user by determining whether the current random one-time code is associated with the user who is identified by the static number. In some embodiments, the random one-time code is discrete and constantly changing with each change from one period of time to the next.

It should also be appreciated that the system illustrated in and described with reference
10 to FIG. 7 can be employed with any embodiment described herein in which the USR is employed to authenticate identity (using either an identification process or a verification process) based on receipt of a random (or pseudo random) one-time code.

Referring now to FIG. 8 a system 670 includes a POS system 672 and a mobile device
15 674. According to some embodiments the mobile device 674 can include a wireless device, for example, a tablet computer, netbook computer, laptop computer, a mobile phone, a PDA, a smart card, electronic passport and the like.

In accordance with some embodiments, the POS system 672 includes a POS terminal
20 676, a credit/debit card interface 678, and a barcode reader 680. Further, according to some embodiments, the POS system 672 includes a communication interface 681 which can include a wireless communication device and/or a hardwired communication device. In accordance with various embodiments, the system element of the POS system 672 can include conventional system elements such as a conventional POS terminal, conventional credit/debit card interface and a conventional barcode reader. In various embodiments, the system 670 can include more or fewer elements than those illustrated in FIG. 8. However, in addition to any of
25 the preceding, the POS system 672 includes an interface device 682 which is integrated with the POS system 672. In accordance with some embodiments, the interface device 682 includes a processor 684, a memory 686, a display 688, a user interface 690, a wireless interface 692 and a hardwired communication interface 694.

- 32 -

In accordance with some embodiments, the interface device 682 operates to allow a registered user of the USR in possession of the mobile device 674 to conduct transactions using the USR and the conventional POS system elements. For example, the mobile device 674 can be used by the user to conduct a transaction in the manner illustrated and described with reference to FIG. 4.

In accordance with some embodiments, the interface device 682 is employed by an operator of the POS terminal of the POS system 672, for example, a cashier or service person. Further, in some embodiments the POS terminal 676 includes a cash register as is traditionally found in a retail establishment.

In accordance with various embodiments, the credit/debit card interface 678 can include a magnetic stripe card reader or other means by which account information is traditionally provided by the credit/debit card holder to the point-of-sale system. Thus, in some embodiments the credit/debit card interface can include a wireless interface that can, for example, communicate wirelessly with a smart card. However, as indicated here, these traditional credit/debit card interfaces may not always be configured to allow a user of a mobile device 674 to take advantage of the functionality and greater security provided by the USR for financial transactions even where the mobile device 674 includes a smart card. Thus, the interface device 682 provides transitional hardware and software to allow the user of the mobile device 674 to take advantage of the functionality and increased security provided by the USR. These advantages are also beneficial to the operator of the POS system 672 because they provide a higher degree of security for financial transactions that are conducted using the POS system 672. The increased security can be provided as described herein by using the USR and the mobile device in an identification process rather than a verification process to authenticate the user of the mobile device 674 and to confirm their credit worthiness.

In accordance with one embodiment, the processor 684 includes a memory 686 while in accordance with other embodiments at least some of the memory 686 is external to the processor. In accordance with some embodiments, a microcontroller is included in the

- 33 -

interface device 682 where the microcontroller includes the processor 684 and at least some of the memory 686.

Further, in accordance with some embodiments, the display 688 includes an LCD display that can be employed by either or both of the operator of the POS system 672 and the user of the mobile device 674 to display information. The user interface 690 can include a touch screen integrated in the display 688 that employs icons or other graphical symbols to allow operation of the interface device 682 to facilitate processing of the financial transaction.

In accordance with various embodiments, the interface device 682 includes any one or any combination of wireless communication protocols and associated hardware including any of Wi-Fi communication 695, near field communication (NFC) 696, GSM (or other cellular communication protocols) 697 and Bluetooth communication 698. In accordance with various embodiments, one or more of these wireless communication protocols can be employed to communicate between the interface device 682 and the mobile device 674 as well to communicate between the interface device 682 and the USB. In other embodiments, alternate forms of wireless communication protocols and/or hardware can be employed in the system 670. According to some embodiments a first wireless network included in the wireless interface 692 is employed to communicate locally between the mobile device 674 and the interface device 682 while a second of the wireless networks 692 is employed to communicate between the interface device 682 and the USB. In further embodiments, a wired communication network is connected to the communication interface 681.

In general, the interface device 682 operates to receive and display transaction information concerning the transaction being conducted between the user of the mobile device 674 and the operator of the POS terminal 676 by, for example, displaying transaction details, authentication requests, approvals, and the like to either or both of the user of the mobile device 674 and the operator of the POS system 672 on the display 688. Thus, in some embodiments the interface device 682 receives the information that is generally provided to the credit/debit card interface 678 concerning the transaction such as the total transaction amount, the cost of individual items being purchased, account information concerning an account of the

- 34 -

user of the mobile device, merchant identification and current time and date. In some embodiments, this information is received and displayed at the interface device 682 and also at the credit/debit card interface 678 in the traditional manner, however, where the USR is employed the interface device 682 can operate to take the place of the credit/debit card interface 678. For example, the interface device can receive the information necessary to
5 authorize and complete the transaction from the mobile device 674. In one embodiment, the electrical connection of the interface device 682 to the POS terminal 676 can be completed by connecting the interface device 682 in series between the POS terminal 676 and the credit/debit card interface 678. According to this embodiment, signals are transmitted from the POS
10 terminal 676 to the interface device 682 and are then communicated to the credit/debit card interface 678. According to another embodiment, the interface device 682 is connected in parallel with the credit/debit card interface 678 such that communication of data from the POS terminal 676 occurs with the direct receipt of the information by each of the credit/debit card interface 678 and the interface device 682.

15 In operation, and in accordance with one embodiment, a user of the mobile device 674 activates the mobile device 674 for conducting a financial transaction such as a purchase of an item at a retail or other commercial establishment. In accordance with one embodiment, the device is activated in the manner illustrated and described at acts 462 to 466 of FIG. 5. That is, the user first enters a PIN in the mobile device and communicates it to the USR. Following a
20 receipt of the PIN by the USR a multi character numeric value is communicated to the mobile device and the user's spoken input of the numeric value is employed to authenticate the user and activate the device for the transaction. In accordance with one embodiment, the communication between the mobile device 674 and the USR to activate the mobile device 674 is conducted without employing the interface device 682. Thus, in accordance with one
25 embodiment, the communication is over cellular network or other wide area network between the mobile device 674 and the USR.

Once the mobile device 674 is activated, the communication link can be established between the mobile device 674 and the POS system 672. In general in these embodiments, a

- 35 -

wireless communication link is established between the mobile device 674 and the POS system 672 via the interface device 682. The user or an operator of the POS terminal 676 can employ a barcode reader 680 or other conventional means to enter information that identifies the item or items being purchased into the POS system 672. The POS terminal 676 receives the
5 information concerning the selected item or items and processes it in a conventional manner to provide a total transaction amount.

In accordance with one embodiment a transaction summary is communicated to the user's mobile device for display, review and approval. In some embodiments, the transaction summary is communicated via the interface device where it may it also be displayed using the
10 display 688. This provides the user with an opportunity to review and if agreed, accept the transaction and request authorization from the USR to execute the transaction. In accordance with one embodiment, the USR application provided on the mobile device 674 allows the user to select an acceptance key or icon to indicate their agreement with the transaction, see for example, act 474 in FIG. 5. In accordance with further embodiments, the mobile device 674
15 using the USR application operates to generate a random one-time code and communicate the random one-time code to the USR along with all or some of the transaction details. As is described with reference to FIG. 5, the USR performs a code matching algorithm to identify the user by locating a match between the USR calculated code included among a plurality of codes calculated for a plurality of users, respectively, and the code generated by and
20 communicated from the mobile 674. According to some embodiments, the communication between the mobile device 674 and the POS and the USR can be completed at this stage using the information provided from the POS system 672 but without the need to communicate directly between the POS terminal 676 and the USR. However, successful completion of the code matching algorithm and check for the credit worthiness of the user of the mobile device
25 674 results in the USR communicating an approval back to the merchant and/or operator of the POS system 672. In a further embodiment, an acknowledgement of the transaction-approval is also provided to the mobile device from the USR. According to some embodiments, the receipt of this information occurs at the interface device 682 where it is displayed to the

- 36 -

operator of the POS terminal 676. According to another embodiment, the communication from the USR of the acceptance or denial of the transaction is communicated to one of the conventional elements included in the POS system 672, for example, the POS terminal 676.

In some embodiments, the mobile device 674 communicates the random one-time code to the POS system 672. According to these embodiments, the POS system 672 combines the code with information concerning any or all of the selected products and prices and a merchant account code. The combined information is communicated from the POS system 672 to the USR. Here too, a successful completion of the code matching algorithm and check for the credit worthiness of the user of the mobile device 674 results in the USR communicating an approval back to the merchant and/or operator of the POS system 672.

According to further embodiments, the USR can be employed to provide apparatus, systems and methods to conduct financial transactions between parties directly, securely and with greater convenience than current approaches. Further, in various embodiments, these approaches provide increased security relative to known approaches by eliminating the necessity to communicate any of, or at least any one of, account numbers, user names, PIN numbers or passwords. In addition, some embodiments are employed in mobile devices that allow flexibility in where and how these approaches are employed. For example, in various embodiments the secure financial transactions can be conducted with a user's mobile device at vending machines, parking meters and at a variety of other locations. Further, the approaches described herein can be employed even in situations in which the parties to the transaction (for example, two users employing mobile devices) are not in communication with the USR at the time of the transaction and/or not in close proximity to one another.

According to one embodiment, two users, each registered with the USR and each having a funds transfer account, in close proximity to one another, intend to conduct a transaction that will result in a transfer funds between their accounts. Each user independently activates their respective mobile device, for example, using the approach illustrated and described concerning acts 462-466 of FIG. 5. According to some embodiments, the device activation includes multifactor authentication in which a biometric is employed. Further, in

- 37 -

some embodiments, the current seed provided from the USR is used in combination with the biometric to activate the device. In some embodiments, the activation of the two mobile devices can include separate authentication protocols such that the user of a first mobile device is identified in a multi-factor authentication process that does not employ a biometric and the user of a second mobile device is identified in a multi-factor authentication process that does include a biometric.

According to a further embodiment, the mobile devices can store default values which can be employed in a financial transaction. The default values can be used to allow a more rapid completion of the transaction by reducing the amount of data that must be entered by the user of the mobile device.

In some embodiments, the two users select the “Funds Transfer” application via the user interface of the respective mobile devices, for example, by using a keypad (a soft keypad, a pushbutton-style keypad, etc.) or an icon located in a graphical user interface displayed at the mobile device. Once the two users have opened the applications, the payer-user enters the amount of the transfer. According to some embodiments, the payee-user then presses a “receive” control element (GUI icon, pushbutton etc.) which is available at the payee’s mobile device via operation of the funds-transfer application. According to some embodiments, the payer-user presses a “send” control element (either alone or in combination with the payee-user pressing the “receive” control element) which is available on their mobile device via operation of the funds-transfer application.

Communication is opened between the two mobile devices and data is exchanged. According to the embodiment, a selected one of a variety of wireless communication protocols can be employed. These may include Bluetooth, NFC, or infrared or other optical or RF signals depending on the embodiment.

According to another embodiment, the mobile devices each include an accelerometer, shock switch or other shock sensor such that communication between the two devices can be initiated when the two users bring the two mobile devices into contact with one another. For example, the two mobile devices can be “bumped” into one another (directly or indirectly, for

- 38 -

example, via contact between the users' hands) so that the transmitted shock/vibration acts on each to open communication via the funds-transfer application. In addition, the preceding can be employed in combination with other user acts such as a selection of an icon in the display of the user's mobile device.

5 In some embodiments, the two devices can remain in communication for completion of the funds-transfer authorization via the USR. According to one approach, the user-payer employs the mobile device to generate and communicate to the USR a first random one-time code that is employed by the USR to identify the payer. Further, the user-payee employs their mobile device to generate and communicate to the USR a second random code that is
10 employed by the USR to identify the payee. The USR can separately employ a code-matching algorithm, as described herein, to perform the identification of the parties to the transaction.

 In general, at least the payer includes the transaction amount in the communication with the USR while in a further embodiment, each of the payer and the payee communicate the agreed upon transaction amount to the USR. According to this later embodiment, the
15 transaction amounts must agree for the transaction to proceed.

 According to some further embodiments, the USR separately authenticates itself to the two mobile devices employed in the transaction by generating a subsequent random one time code based on a seed associated with the respective mobile device and the current time. The one time random code generated by the USR for the user-payer is communicated to the payer's
20 mobile device and the one time random code generated by the USR for the user-payee is communicated to the payee's mobile device. The two mobile devices each employ their respective seed with the time that the USR generated the random one-time code to confirm the identity of the USR.

 The USR can communicate (subsequent to or along with the communication of the
25 respective random codes) a digital image of the payer to the payee and a digital image of the payee to the payer. Further, for added security, the USR can transmit multiple images (for example, a "line-up" of images) of a plurality of individuals to the two parties and the funds transfer is not finalized until the payer accurately selects the image of the payee and the payee

- 39 -

accurately selects the image of the payer from among the respective plurality of images which are received. Security of such an approach can be increased by allowing each of the parties only one or some other limited number of selections in which to accurately identify the correct image.

5 The parties communicate via the respective mobile devices the confirmation of the visual identity of the other party to the USR which then operates to transfer (for example, electronically transfer) the requested amount of funds from the payer's account to the payee's account.

10 According to some embodiments, a funds transfer can also be completed between a payer and payee even where the two parties are not in proximity with one another. According to these embodiments, the payer activates their mobile device and selects the funds transfer application. The payer then enters an identifier that identifies the payee such as the payee's mobile phone number, the payee's email, etc. along with the amount of the transfer. The payer communicates with the USR and transmits a one-time random code that the USR employs to
15 identify the user. The USR identifies itself to the payer by transmitting a subsequent random one-time code based on the seed associated with the payer's mobile device and the current time. According to this embodiment, the payer confirms the identity of the USR based on the received one-time random code. In some embodiments, the payee is identified by the USR and the payee confirms the identity of the USR in a similar manner. Here too, the USR can
20 communicate a digital image of the payee to the payer and an image of the payer to the payee for increased security. Provided that the preceding identity-process is successfully completed, in some embodiments, the payer can then select the "pay" soft-key provided by the funds transfer application.

25 According to another embodiment, the USR and a mobile device of a registered user with a funds transfer account can be employed by the user to conduct transactions (for example, make purchases) at a vending machine, self service check out, unmanned-kiosk and the like. According to these embodiments, the owner or proprietor of the unmanned system is also registered with the USR and has an account that includes the funds transfer option.

- 40 -

According to this embodiment, the payer opens the funds transfer application as previously described and communicates with the unmanned system to conduct a transaction. Information concerning the transaction such as the selected item, the cost, sales tax (if any), the identity of the parties and the like can be communicated. According to one embodiment, the owner or
5 proprietor is a corporation or other business entity. According to this embodiment, the logo of the business entity is communicated to the mobile device for display to the user. The user can visually confirm that they are dealing with the correct business entity and then enter the amount of the transaction and accept the purchase by selecting the appropriate soft-key generated by the funds transfer application.

10 According to some embodiments, the funds transfer described in the preceding paragraph is completed using an authentication process with the USR on a substantially real-time basis. For example, the identity of the payer can be performed as described above prior to the payer receipt of the item. Where real-time communication between the mobile device and the USR is unavailable for the transaction, the actual funds transfer is completed at a later point
15 in time as described below.

According to any of the preceding embodiments, execution of financial transactions (including purchases, etc.) approved and authorized by a payer and a payee can be deferred if the two parties are not in communication with the USR at the time the parties agree to the transaction. The completion of the transaction including the communication of the random
20 one-time codes, successful identification of the USR and cross-identification by the parties can be separately completed by the payer and the payee when they are next in communication with the USR. The USR can defer the transaction until each of the two parties completes the parts of the transaction for which they are responsible. According to some embodiments, the communication between the users' mobile devices and the USR is automatically established
25 when such communication is next available.

Referring now to FIG. 6, a process 500 is illustrated by which users can employ their mobile devices for use in a personal payment transaction, or other types of interactions during periods where the user devices are in communication with USR. The process generally

- 41 -

includes the authentication of the users by their respective devices, for example, by their mobile devices. The process 500 may, in some embodiments, also include communication between the two devices, for example, wireless communication between the two devices. However, in other embodiments, communication between the two devices is not employed. In
5 some embodiments, identities of each of the two users are authenticated by USR. In other embodiments, USR authenticates an identity of only one of the two users, for example, the payor. Further, in some embodiments, USR authenticates itself to either or both of the devices via a “handshake” process as described below.

The approaches described herein generally employ multi-factor authentication.
10 According to some embodiments, the approaches employ 3+ factor security. As referred to herein 3+ factor security employs each of something the user knows, something the user has, and something the user is, and in addition, employs one of the preceding three factors more than once. Such approaches are described in greater detail herein.

Referring to the process 500, at Act 502, user #1 is authenticated by their mobile device
15 (Device 1). Similarly, at Act 504, user #2 is authenticated by their mobile device (Device 2). According to some embodiments, the process 500 includes Act 506 in which Device 1 and Device 2 establish a communication protocol with one another. The communication protocol may allow the wireless exchange of identifying information (for example, public identifying information) for each of user #1 and user #2. For example, Device 1 can transmit a public ID
20 of user #1 to Device 2 while Device 2 transmits a public ID of user #2 to Device 1. Act 506 is identified as optional because, according to some embodiments, the process 500 is completed without any direct communication between Device #1 and Device #2.

Although the current embodiment is described with reference to a financial transaction that involves user #1 and user #2, the approaches described herein may be employed by two or
25 more parties to authorize (and/or agree to) a variety of actions. According to these embodiments, the user selects an identity of the other party(ies), the agreed upon act, and if necessary, any other details, constraints or qualifiers. As will be apparent to those of ordinary skill in the art, the party identification is in the form of something other than a “payee” or

- 42 -

“payor” where the action does not involve a payment. Further, regardless of the form of transaction the identification of the parties to the transaction can include the identification of an entity such as a company or other organization rather than an individual.

According to one embodiment, at Act 508 user #1 selects each of the payee and an amount of a financial transaction. Further, user #1 can also select, at Act 508 an amount of the transaction and/or an account type (or other identifier) suitable with the selected transaction.

According to this embodiment, user #1 can select/enter the payee identification using data stored in the mobile device or by manually entering the ID information in the device. According to one embodiment, the identifying information of user #2 is located in the contact or address book in Device 1. Therefore, depending on the embodiment, the identifying information of user #2 can be provided by user #1 in the form of any of a name, a shorthand identification, an email address or phone number of user #2 which is selected from the contacts stored in Device 1. Alternatively, where the process 500 includes the Act 506 the payee identification can be provided to user #1 by transmission from Device 2 to Device 1. Similarly, at Act 510 user #2 selects each of a payer (user #1) and an amount of the financial transaction.

In some embodiments, the information selected by user #1 is communicated to USR at Act 512 (for example, wirelessly transmitted). In addition, Device 1 can be employed to generate a non-predictable value, as described elsewhere herein, that is used to authenticate the identity of user #1 at USR. In the illustrated embodiment, the transmission of the non-predictable value is included in Act 512. According to other embodiments, the non-predictable value is transmitted in a separate act that precedes Act 512. In addition, Act 512 can be preceded with a step or series of steps included in the process 500 in which USR authenticates itself to the device. For example, as illustrated in the process 580 of FIG. 10.

At Act 514, user #2 employs Device 2 to generate and communicate a transaction request/authorization to USR in a similar manner to that described with reference to Act 512. Here too, a non-predictable value can be communicated from the user’s device (Device 2) to USR along with the payer ID and the dollar amount of the transaction. Further, according to

- 43 -

some embodiments, Device 2 can be employed to generate a non-predictable value, as described elsewhere herein, that is used to authenticate the identity of user #2 at USR. In addition, Act 514 can be preceded with a step or series of steps in which USR authenticates itself to the device. For example, as illustrated in the process 580 of FIG. 10.

5 At Act 516, USR authenticates identities of user #1 and user #2, respectively. According to various embodiments, Act 516 can include one or more additional acts. For example, provided that the authentication of user #1 is successful, USR can also check the availability funds for the requested transaction.

10 At Act 517, where the authentication of either or both of user #1 and user #2 is unsuccessful or the necessary funds are unavailable USR can communicate the fact to either or both of user#1 and user #2. According to some embodiments, the process 500 ends where at least one of the authentications is unsuccessful. In some embodiments, following act 517, the process 500 can include a subsequent attempt to complete the transaction by either or both of user #1 and user #2.

15 According to further embodiments, execution of the transaction can also require confirmation by the respective users of the identity of the others. For example, as illustrated in FIG. 6, at Act 518 USR transmits an image of the payer (user #1) to the payee (user #2) and an image of the payee to the payer for local authentication of identity by the parties to the transaction. According to this embodiment, an image of the payer (user #1) appears on display
20 of Device 2 and an image of the payee (user #2) appears on a display included in Device 1.

 According to this embodiment, USR defers executing the transaction until the users accept the identity of one another based on the image, see Act 520. For example, where user #1 accepts the identity of the displayed image of user #2 and communicates acceptance to USR (for example, by selecting a key or icon included in the display of Device 1) and user #2
25 confirms the identity of user #1 in the same manner using Device 2. In accordance with some embodiments, only one of the two parties to the transaction receives an image of the other. In accordance with still other embodiments, neither party receives an image of the other, for

- 44 -

example, the process 500 does not include Act 518. Here too, the process can terminate where
USR does not receive either or both of the acceptances.

According to some embodiments, the process 500 does not include Act 506. Instead,
the mobile devices of the two users do not directly share any information with one another.

5 According to this embodiment, Device 1 communicates identification of the payee in the form
of the identification selected from data included in the mobile device or manually entered by
user #1. User #2 can employ the same approach using Device 2 to identify the payor.

Referring now to FIG. 9, a process 540 is illustrated where a transaction is initiated by
two users in situations in which either or both of the associated devices is not in
10 communication with USR. This is sometimes referred to as an out-of-band transaction. At Act
542, Device 1 authenticates user #1 and at Act 544, Device 2 authenticates user #2. Either of
Act 542 and Act 544 can be accomplished as described elsewhere herein by local
authentication of the user, respectively (for example, by the user's mobile device).

At Act 546, the devices open a communication protocol with one another to initiate the
15 transaction by, for example, exchanging public ID information as described concerning Act
506 illustrated in FIG. 6. According to other embodiments, the process 500 does not include a
direct communication between the two devices and the mobile devices of the two users do not
directly share any information with one another. Instead, the public ID info is provided to the
USR by the respective user as described with reference to the process 500.

20 At Act 548, user #1 selects each of a payee and an amount of the desired financial
transaction. Similarly, at Act 550, user #2 selects each of the payer and an amount of the
financial transaction.

Although the current embodiment is described with reference to a financial transaction
that involves user #1 and user #2, the approaches described herein may be employed by two or
25 more parties to authorize (and/or agree to) a variety of actions. According to these
embodiments, the user selects an identity of the other party(ies), the agreed upon act, and if
necessary, any other details, constraints or qualifiers. As will be apparent to those of ordinary
skill in the art, the party identification is in the form of something other than a "payee" or

- 45 -

“payor” where the action does not involve a payment. Further, regardless of the form of transaction the identification of the parties to the transaction can include the identification of an entity such as a company or other organization rather than an individual. As will also be apparent, where the action/permission to be agreed upon does not include a payment, the
5 respective parties can provide USR with a description concerning the requested action, for example, access to a particular physical space or secure electronic system during a specific time-period and/or for an agreed upon cumulative amount of time.

In the illustrated embodiment, where Device 1 is not in communication with USR, the authentication of user #1 and processing of the payment request is delayed until such time that
10 Device 1 can communicate with USR. Similarly, where Device 2 is not in communication with USR, the authentication of the identity of user #2 and the processing of the payment is deferred until such time that Device 2 is in communication with the USR. Accordingly, the transaction is not completed until each of Device 1 and Device 2 are in communication with USR, subsequent to acts 548 and 550, such that remaining acts included in the process 540 can
15 be completed.

For example, where Device 1 is not in communication with USR at the time user #1 requests the transaction then the non-predictable value associated with user #1 is transmitted to USR along with a payee ID and the dollar amount of the transaction when Device 1 is next in communication with USR. Similarly, at Act 554, where Device 2 is not in communication
20 with USR at the time user #2 requests the transaction then the non-predictable value associated with user #2 is transmitted to USR along with the payer ID and the dollar amount when Device 2 is next in communication with USR. As described with reference to the process 500 of FIG. 6, either or both of the acts 552 and 554 can be preceded by an authentication of USR to the respective mobile devices, for example, as illustrated in acts 586 to 590 of the process 580 in
25 FIG. 10.

At Act 556, USR authenticates the identity of the payer (user #1) using the non-predictable value received from Device 1 while at Act 558 USR authenticates the identity of the payee (user #2) using the non-predictable value communicated from Device 2.

- 46 -

At Act 560, where USR successfully authenticates the identities of both payer and payee, the request is processed. Alternatively, should authentication of at least one of the parties to the transaction fail USR will not complete the transaction but will instead notify the parties that the request cannot be processed, at Act 561. Where the transaction is completed
5 successfully, USR transmits confirmation to the payee and payer at Act 562.

Referring now to FIG. 10, a process 580 is illustrated including multi-factor security where the factors include each of something the user knows, something the user has, and something the user is. The use of one of the preceding factors more than once in an authentication process (in the same or different form) adds an additional level of security that
10 provides 3+ security. For example, in some embodiments, a first form of biometric is included in the original three factors that are authenticated (for example, voice recognition) and a second form of biometric (for example, an image) must also be authenticated to allow the action (for example, a financial transaction) to proceed. According to some embodiments, the respective factors may be authenticated by the same elements or different elements included in
15 the process. For example, one or more factor can be authenticated for device activation, while the same or different factor(s) are authenticated by USR. In a further embodiment, the same or different factors for the same user or entity are authenticated by a third party, for example, an operator of a POS or a party to a personal payment.

At Act 582, a user's device authenticates the user based on a biometric input. The
20 biometric input can be any of the variety of biometric inputs described herein including voice, fingerprint, handwriting, retinal scan or any other form of biometric that can be sensed and processed by the device. Although illustrated as authentication using a biometric, other forms of device-based user authentication can be used in accordance with various embodiments.

At Act 584, the user enters a PIN in the device. Further, the PIN is employed along
25 with the time and the seed which was previously provided to the device by USR to provide a non-predictable value, NPV #1. As will be recognized, the non-predictable value includes a time-varying value where time is employed in the derivation of the NPV #1. At Act 586, the process continues with all or a portion of NPV #1 being transmitted to USR for an initial

- 47 -

identification of the user in possession of the device. According to one embodiment, the non-predictable values generated in the process 580 are 20 digits or more. However, the number of digits (either generated or transmitted) can be adjusted in advance to achieve a desired level of security.

5 For example, Act 586 can include a transmission of a complete 20+ digit non-predictable value. Alternatively, only a portion of the 20+ digit non-predictable value can be transmitted from the device to USR for an initial identification (that is only a subset of digits generated are submitted). In some embodiments, a generation and/or transmission of a non-predictable value having a smaller size can increase the efficiency and speed at which the
10 process 580 is completed. Then, at Act 587, USR employs the transmitted non-predictable value to determine an identity of the user associated with the device. In various embodiments, one or more of the code matching approaches described herein can be employed at USR in Act 587.

Should the initial identification using NPV #1 fail, the process can also include an Act
15 589 in which the USR notifies the user that the identification failed. According to some embodiments, the user may get an opportunity to provide another NPV #1 to USR to initially establish their identity.

At Act 588, USR, using the time and the seed associated with the device, determines the next non-predictable value in sequence that would be generated by the device. The USR
20 generates this next-in-sequence non-predictable value (NPV #2) and transmits it to the user device. Here too, can include a transmission of a complete 20+ digit non-predictable value. Alternatively, transmission of the non-predictable value can include all or only a portion of a 20+ digit non-predictable value (again, only a subset of digits generated are transmitted). Considerations here include the desired level of security, the processing power included in the
25 user's device and the associated amount of time required for the device to perform the comparison required to authenticate USR.

Should the validation of the USR fail, the process can also include an Act 591 in which the USR receives notification that the validation at the user device was unsuccessful.

- 48 -

According to some embodiments, the USR the same or a different NPV#2 subsequent to Act 591.

At Act 590, the user device validates USR based on NPV #2. For example, user device can employ the seed and the time of the time increment at which NPV#2 was generated to
5 determine the value that is generated by an authentic USR. The user device compares NPV#2 to this value to determine whether the device is in communication with USR rather than an imposter (to detect man-in-the-middle attacks). Provided that USR is successfully authenticated by the device, the process 580 proceeds to Act 592.

At Act 592, the user device generates NPV #3 using at least the time and the seed
10 associated with the device and transmits NPV #3 to USR. In this instance, the full 20+ digit non-predictable value is transmitted in its entirety to provide a high level of security. In addition, as illustrated at Act 594, NPV #3 can be combined with information identifying the recipient of funds involved in the transaction as well as an amount of the transaction before being transmitted. In one example, NPV #3 is XORed with the information regarding the
15 recipient of the funds and the amount. Further, in some embodiments where lower security is acceptable, act 592 includes transmission of fewer than 20 digits to increase the speed of the process 580.

At Act 596, USR authenticates the identity of the user based on the non-predictable value transmitted from the user device (NPV #3). In addition, USR can check for the
20 availability of funds in the user's account.

Should the authentication fail, the process can also include an Act 597 in which the USR notifies the user that the authentication failed. According to some embodiments, the user may get an opportunity to try a subsequent authentication attempt with USR at Act 597.

At Act 598, USR processes the transaction provided that the identity of the user is
25 properly authenticated and that the available funds are sufficient to cover the requested transaction. USR can notify a selected party or party to the transaction should the authentication and/or financial check fail.

- 49 -

According to alternate embodiments, the USR acts as an intermediary to banks, credit card companies or other financial service entities. According to these embodiments, the USR communicates the transaction details to the financial services company. The approval or denial of the transaction is then communicated to the user either directly from the financial services
5 company or via USR, depending on the embodiment.

In addition, in some embodiments, an image of the user can be transmitted to either the user's device (to allow the user to display the image to another party to the transaction) or directly to the device of the other party for display. According to these embodiments, USR defers the processing described at Act 598 until receipt of an acknowledgement by the party
10 who has responsibility for review of the image authenticating the identity of the user.

In this or any other embodiment in which an image of a first party to a transaction request is displayed for review by a second party, the selection of the image that authenticates the identity of the first party can be a pre-requisite to the completion of the transaction. For example, as described herein with reference to Act 518 and 520 of FIG. 6 or Act 486 of FIG. 5.
15 Further where embodiments include such an act at a point-of-sale, a clerk or other staff-member can select the image from among a plurality of images that are displayed at the POS terminal (for example, the POS terminal 676 or the interface device 682 illustrated in FIG. 8). In one approach, each of a plurality of customers has established wireless communication with the POS terminal or interface device and an image of each is displayed to the clerk. The clerk
20 selects the image of the customer who is currently conducting the sales transaction. For example, the clerk can select the image of the user with a touch-screen included for the POS (either a fixed location POS or a portable tablet-type POS).

Further, where the close proximity of multiple individuals/parties requires a selection of a unique party to the transaction from among a plurality of possible parties, a customer can
25 enter a unique POS identifier to either initiate or complete a selected transaction. For example, the user enter the number associated with a particular check out station/line, gas pump, etc. According to some embodiments, a proximity signal is employed to restrict transactions to

- 50 -

only those wireless user-devices that are located immediately adjacent to the POS, or the wireless user device of the other party.

According to various embodiments, the non-predictable values employed in the process 580 are random one-time numbers, for example, pseudo random numbers. Further, according to some embodiments, the non-predictable values used to identify the user to USR (for example, at act 586) and to identify the USR to the user (for example, at act 588) are a partial (or subset of digits) from a non-predictable value generated for a previous time period for the user that were not employed for authentication. For example, the NPV #1 and the NPV #2 are previously generated but unused random one-time numbers, or portions thereof. Further, the preceding embodiments can be used where the USR is a "cloud" resource available to the user. According to some embodiments, the USR receives a first portion of NPV#1 from the wireless user-device where the first portion is employed by the USR to identify the wireless user-device to the USR. Prior to authenticating the identity of the user but with a high degree of certainty that it is communicating with an authorized user-device, the USR transmits a second portion of the NPV#1 to the user-device. Thus, the second portion of NPV#1 is employed as NPV#2 in the process 580. Where the second portion matches the value expected (generated as a portion of NPV#1) by the user-device, the user-device has a high degree of certainty that user-device is communicating with the USR rather than an imposter to complete the authentication process (for example, the authentication process 580 beginning at 592).

According to some embodiments, an untransmitted portion of a previously generated non-predictable value may be employed as an exclusive-or (XOR) checksum to insure the integrity and authenticity of the information being transmitted. Similarly, previously generated but unused non-predictable values can be used to encrypt (for example, using an exclusive-or operation) data communicated from either the user-device or the USR.

Further, in various embodiments, the random one-time code (for example, any of NPV#1, NPV#2 and NPV #3) is generated by employing a PIN in combination with any one of or any combination of an electronic serial number of the user-device, a SIM number of the user-device and a seed associated with the device. According to one embodiment, the PIN is

- 51 -

stored in the user-device while in an alternate embodiment the PIN is not stored in the user-device.

Referring now to FIG. 11, a system 650 including a USR 654 and a plurality of wireless user devices 652 (for example, wireless tokens 1-N) is illustrated in accordance with one
5 embodiment. As used herein, the term “token” refers to a device that represents at least one factor employed in authenticating an identity of a user or entity. As should be apparent, in some embodiments, a token can include a mobile user device such as a mobile phone where the token represents something the user has. For example, the token can include a seed that must be employed to generate authentication information that can be successfully processed by
10 the USR 654. In the illustrated embodiment, the system 650 can also include one or more network access devices 658, depending upon the embodiment, and a network 656. In general, the system 650 can be employed by a user in possession of a wireless token such as a smart phone, tablet or other form of wireless electronic device. According to various embodiments, the network 656 provides users with access to the cloud where a variety of remote resources
15 (for example, the USR 654) can be accessed.

In the illustrated embodiment, each of the wireless user devices 652 include a biometric sensor 602, a user interface 604, a wireless transceiver 606, a processor 608, a display 610, a memory 612 and a power source 614. According to one embodiment, the display 610 is
20 included in the user interface 604. In various embodiments, the biometric sensor 602 can detect at least one of a voiceprint, a fingerprint, a signature and a retinal scan. Further, one or more communication busses can be included in the wireless user device 652 to a communication of electronic signals within the user device such as the communication of data and/or instructions. The processor 608 can, for example, control communication within the user device 652. According to some embodiments, the processor is included in a
25 microcontroller.

In some embodiments, the system 650 includes all or some of the features and functionality described with reference to the system 730 illustrated in Fig. 12. For example, the wireless networks and wireless communication protocols employed for communication

- 52 -

between the wireless user devices 652 and/or between the user devices and the network access device 658 can include any of those identified with reference to the system 730. As another example, the wireless device 652 can include all or some of the features and functionality described with reference to the wireless user device 735 of the system 730 illustrated in FIG.

5 12. For example, the wireless user device 652 can include any of the seed 757, the SIM 758 and the ESN 759 illustrated in FIG. 12. Further, in some embodiments, the USR 654 includes all or some of the features and functionality of the USR 734 of the 730 illustrated in FIG. 12.

In various embodiments, the system 650 can also be employed as a peer-to-peer secure identification system. According to one embodiment, biometric information for a pre-defined affinity group (for example: U.S. air marshals; FBI, CIA, Secret Service, Homeland Security or 10 TSA personnel; airline employees, members and/or employees of Congress, the White House, the Pentagon, Fortune 500 companies, private organizations or the armed services) is maintained by the system. The system 650 allows members of the affinity group to challenge and/or identify themselves to one another in a highly secure manner with a high degree of 15 certainty that the authentication information that is presented is legitimate. According to some embodiments, the wireless user-device 652, for example, the wireless user-device 652 of a challenger is stationary rather than a mobile device.

In general, authorized individuals register and establish their secure account at the USR 654 (see, for example, approaches described with reference to FIGS. 1-3, herein). In some 20 embodiments, their digital photograph or other biometric information is obtained and stored in the database included in the USR 654. Other members of the affinity group register similarly and an affinity group manager establishes the members of the group. In one embodiment, the affinity group manager directly manages the membership on the USR server(s). According to another embodiment, the manager contacts the business entity that operates the USR 654 and 25 that organization implements the necessary change(s) in membership status. In some embodiments, a different type of biometric is employed either alone or in combination with the image in an authentication process.

- 53 -

The stored biometrics and/or images are used as described below to authenticate identity. According to these embodiment, each of the user devices 652 stores a first portion (the A portion) of the biometric, respectively, of all members of the affinity group (with the possible exception of themselves). The user device 652 stores a second portion (a B portion) of the biometric of the user associated with the user device 652.

In a further embodiment, when two members of an affinity group meet they employ their respective user devices 652 and stored biometric information to authenticate one another. In one embodiment, a first user wirelessly transmits the B-portion of their biometric to the user device 652 of a second user. The user device 652 of the second user receives the B-portion for the first user and combines it with the previously stored A-portion for the first user to provide the full biometric for the first user. The second user then reviews this “full” biometric of the first user to authenticate the first user. According to one embodiment, the biometric includes an image where the A-portion and the B-portion are different portions of the image, for example, they may be different halves. The “full” biometric of the first user can be displayed in a display included in the user device of the second user. Similarly, in some embodiments, the second user also wirelessly transmits the B-portion of their biometric to the user device 652 of first user. The user device 652 of first user receives the B-portion for second user and combines it with the previously stored A-portion for the second user to provide the full biometric for the second user. The first user then reviews this “full” biometric of the second user to authenticate the second user.

In some embodiments, the biometric is split in half and the first portion and the second portion are halves. However, the biometric need not be split in half. Accordingly, in some embodiments, the percentage of the biometric of other members of the affinity group stored on a user device can be either a higher or lower percentage of the full biometric. Regardless of the split, the combination of the two biometrics need only provide a full biometric in combination with the corresponding portion.

According to some embodiments, the biometric (for example, an image) is divided in a manner that further increases the security of these approaches. For example, an algorithm can

- 54 -

be employed at each of the USR 654 and the user devices 652 to divide the stored images for a particular affinity group in a varying and irregular manner. According to one embodiment, the division is latitudinally (horizontally) so that the first and second portions are upper and lower regions of the image, respectively. According to another embodiment, the division is occurs
5 longitudinally (vertically) so that the first and second portions are left and right regions of the image, respectively. Employing such an algorithm, the two portions of the images provide the A and B portions, respectively, as a ratio of the percentage of the image included in portion A to the percentage of the image included in portion B varies.

In some embodiments, the parties in an affinity group can, using their wireless user
10 devices 652 challenge one another when they meet. In one embodiment, a soft key is selected in a user interface of the mobile device 652. The selection of the identity-application on the user device initiates a Bluetooth handshake in which authentication information is communicated from one device to another. In general, the communication serves to establish to each user that the other user appears to be a registered member of the affinity group, and
15 following that, authenticates their identity. In some embodiments, a proprietary protocol is employed by the devices 652. In one embodiment, such a protocol utilizes asymmetric encryption. A high resolution image of the challenged individual and relevant identifying information (for example, identifying who they purport to be) is displayed on the user device of the challenger. The image is a full image including the A-portion and the B-portion of the
20 image which are assembled by the wireless user device 652 of the challenger.

An approach in which the user devices store the various portions of the biometrics is advantageous because the user devices need not be in communication with USR 654 to perform an authentication. According to these embodiments, access to the network 656 or other network for communication with the USR 654 is not required. Thus, the authentication
25 process can be completed in locations where external network access is unavailable such as, for example, underground locations, "black" facilities, in a plane at 30,000 feet of altitude, on land, sea, or space. However, in other embodiments, the A-halves are not stored on the user

- 55 -

devices 652 but are instead stored at USR 654. According to this embodiment, USR 654 communicates the A-half of a user on request from a member of the affinity group.

Advantages of these approaches include the fact that the approach is rapid. Simple and convenient to use, provides increased security relative to other approaches, is incorporated in an existing item carried by the great majority of people, does not draw attention to the participants when in use, can be field upgradeable with affinity group additions and deletions in substantially real-time where communication with the USR 654 is available, and cannot be used by a third party if lost or stolen.

Further embodiments can also provide any of: control of secure access to classified computers and/or networks; provide secure access to physical facilities, supplement or replace existing less-secure personal ID approaches such as conventional ID badges, ID documentation, drivers licenses, and passports); replace credit cards, toll payment devices, activate/deactivate security alarm systems at home or office; and provide audit trails via, for example, the use of GPS integrated in the wireless user devices 652.

In addition, the system 650 can include the following features in the wireless user device 652: a duress alarm whereby a user can employ the user device 652 to signal the USR 654 that they are under duress without detection by others (for example, where the user adds a known value (+1) to the PIN at the time of entry); and a self destruct mode in which either or both of hardware or software/stored data of the user device 652 is destroyed or rendered inoperable when tampering or abuse of the device is detected. In some embodiments, "self-destruct" can also be triggered based on a passage of time without receiving and/or being able to communicate a reset signal; based on targeted events; or when a location of the user device 652 is out of a pre-defined geographic area. To further increase security, the user device 652 can cryptographically hash data files when not in use.

In some embodiments, the user is challenged by other than an individual with another wireless user device 652. For example, the preceding approaches can be applied to point-of-sale transactions or an access control point. Also, although the above-described approach

- 56 -

describes use of an image as the shared biometric, further approaches can employ any of a fingerprint, a signature, a voiceprint and DNA codes as the shared biometric.

Referring now to FIG. 12, a system 730 employing a Universal Secure Registry (USR) is illustrated in accordance with one embodiment. In the illustrated embodiment, the system
5 730 includes a USR 734, a wireless user device 735, at least one computer 736 and a network 738. In accordance with various embodiments, the wireless user device 735 can include any of a mobile phone, a tablet computer and a personal digital assistant or other type of computing device.

In the illustrated embodiment, the USR 734 includes a user interface 740, a processor
10 742, a communication interface 744 and a database 746. The USR 734 can also be configured with fewer than all of the preceding elements or additional elements alone or in combination with the preceding. For example, the USR 734 can include any of the elements and/or functionality concerning the USR embodiments described herein. Further, the USR 734 can include one or a plurality of servers co-located or in configurations in which one or more of the
15 servers is geographically remote from others of the servers. According to one embodiment, the USR 734 provides a secure centralized registry that can be employed to facilitate a variety of activities, for example, activities in which authentication of identity is required.

In the illustrated embodiment, the wireless user device 735 includes a user interface
20 750, a secure element 751, a memory 753, a processor 752, a wireless transceiver 754, a display 755, a biometric sensor 756, a seed 757, a Subscriber Identity Module (“SIM”) 758 and an electronic serial number 759.

In accordance with various embodiments, the user interface 750 can include any of a keypad, a camera, a microphone and the display 755. In one embodiment, the user interface includes a touch screen graphical user interface.

25 In accordance with various embodiments, the memory 753 can include a plurality of memory devices, for example, RAM, ROM, flash memory, SRAM memory or other memory devices. In one embodiment, the processor 752 is included in a microcontroller that includes the processor and memory. Further, the memory can be a discrete memory component,

- 57 -

integral to the microcontroller or include both a discrete component and memory included in the microcontroller.

In accordance with some embodiments, the wireless transceiver 754 provides a communication interface in which the wireless user device 735 transmits information including authentication information from the device 735. The wireless user device 735 can also include one or more hardwired communication interfaces. As should be apparent, the wireless transceiver 754 can also be configured to receive information transmitted to the wireless user device 735.

According to some embodiments, the seed 757 is distributed in a manner as described herein concerning the embodiments associated with FIG. 7. In some embodiments, either or both of the seed 757 and the electronic serial number 759 are stored in the memory 753. In further embodiments, the seed 757 and the electronic serial number are stored in a region of the memory 753 that is secured in a manner that makes it more difficult to access by unauthorized parties (which may, for example, include the user). According to some embodiments, the secure element includes an electronic component such as one or a combination of a processor, a microcontroller and a memory. In accordance with some embodiments, the USR seed 757 and/or the electronic serial number 759 are stored in the secure element 751.

In accordance with one embodiment, the computer 736 includes a wireless transceiver 760, a user interface 762, a processor 764, a memory 766 and a USR element 768. Further, the system 730 can include one or a plurality of computers, such as the computers 1-N. For example, a single wireless user device may be employed to access each of the plurality of computers. In one embodiment, the plurality of computers can include an office computer, home computer and any number of computers that can communicate with USR and are secured using the system illustrated in FIG. 12. The computer 736 can include a plurality of computers that are geographically remote from one another. In accordance with various embodiments, the computer can include anyone of a desktop computer, a notebook computer, a laptop computer, a netbook computer and a tablet computer. As will be apparent, other styles and types of computers can be employed in the system 730. In accordance with some

- 58 -

embodiments, the computer is a “dumb” terminal that provides access to a network such as a wide area network (the Internet, an intranet or both) that allows an authorized user to access resources (for example, using a web browser) via the computer terminal.

In accordance with various embodiments, the network 738 can include a wide area
5 network, a local area network or a combination of wide area network and a local area network. Further, the network 738 can include wired or wireless networks or combinations of both. Further, according to some embodiment the wireless user device 735 can also communicate over the network 738. In still other embodiments, the wireless user device 735 can
10 communicate with the USR 734 over one or more additional networks that are not employed for communication between the computer 736 and the USR 734.

According to some embodiments, the system 730 is employed as proximity-based computer security system using the wireless user device 735 to generate authentication information to allow a user in possession of the device 735 to unlock the computer 736. According to some embodiments, the wireless user device 735 is employed to provide
15 authentication information wirelessly to the computer when the wireless user device 735 is in proximity of the computer, for example, where proximity is determined by a range of the wireless network. According to these embodiments, the wireless network allows the wireless transceiver 754 of the device 735 to communicate with the wireless transceiver 760 of the computer 736.

20 In various embodiments the wireless network over which the device 735 and the computer 736 can communicate can include any one of Wi-Fi communication, near field communication (NFC) and Bluetooth communication. For the preceding examples, each type of wireless communication has limited range where Wi-Fi communication has the greatest range, NFC has the most limited range and Bluetooth has a range greater than NFC but less
25 than Wi-Fi. Thus, for each of the preceding types of wireless communication the wireless user device 735 and the computer can remain in wireless communication only so long as the device 735 and the computer 736 are in proximity of one another. In further embodiments, other forms of wireless communication can be employed. Further, where the inherent maximum

- 59 -

communication distance is greater than desired, security can be increased by modifying the wireless network hardware or software such that the range is further limited, for example, to a few feet.

According to one embodiment, a user can unlock the computer 736 to access computer
5 resources by successfully authenticating their identity with the USR 734 and then keeping their wireless user device 735 proximate to the computer 736.

In accordance with some embodiments, at least a portion of USR is included in the computer 736. In the illustrated embodiment, the USR element 768 is deployed in the computer 736. The USR element 768 can take various forms depending upon the embodiment.
10 According to one embodiment, the USR element 768 is a software module that performs local authentication of authentication information received from the wireless user device 735. In some embodiments, the USR element 768 includes a combination of hardware and software. Further, where the USR element 768 includes software, the USR element can be electronically-distributed to the computer 736, for example, via the network 738 or via a different network.

In accordance with other embodiments, the USR element 768 only provides an
15 interface between the computer 736 and the USR 734. In accordance with this latter embodiment, communication from the wireless user device 735 is relayed or can be relayed to the USR 734 via the computer 736 using the USR element 768. In still other embodiments, the computer 736 can relay authentication information or other communication from the wireless
20 user device 735 over the network 738 without need for the USR element 768.

In embodiments where USR elements 768 can locally authenticate the user of the wireless user device 735, the USR element can provide it in software such that element 768 can be distributed, for example, securely distributed to a variety of computers 736 that are remote from the USR 734. In accordance with one embodiment, the USR element 768
25 includes a seed for each user authorized to unlock the computer, respectively. According to this embodiment, the complete authentication of non-predictable values provided by users can be accomplished locally by the computer 736. Thus, in some embodiments, authentication, including bilateral authentication, can be accomplished by the computer 736 without any real-

- 60 -

time interaction by the computer with the USR 734. These authentication protocols can include all or some of the acts illustrated in Figs. 33 and 38, where the protocols are employed to allow access to the computer 736 (for example, rather than authorize a financial transaction). Further, automatic seed updates for both the wireless user device 735 and the computer 736
5 can occur as described above with reference to FIG. 7. These seed updates can occur with or without knowledge and/or interaction with the user, for example, they may occur randomly.

According to some embodiments, the proximity-based security provided with the wireless user device 735 in combination with the USR 734 is achieved where a USR element is not included in the computer 736.

10 The overall operation of the system 730 allows the user to operate the computer 736 to access resources using the computer so long as the computer periodically receives authentication information from the wireless user device 735 where that authentication information is successfully authenticated by the USR system either at the USR 734, at the USR element 768, or employing each of the USR 734 and the USR element 768. In some
15 embodiments, a portion of the authentication protocol is performed by each of the USR elements 768 and the USR 734.

Various authentication information can be communicated from the wireless device 735 to the USR to authenticate the user of the device 735 depending on the embodiment. For example, the information transmitted from the wireless user device 735 to the computer 736
20 can include a time-varying non-predictable value. Multi-factor communication protocols described herein can be employed including protocols in which a time-varying non-predictable value is generated as a result of 2, 3 or 3+ factors.

In some embodiments, the protocol includes the generation of an initial time-varying non-predictable value by the device 734. This value is wirelessly communicated to the
25 computer 736 for authentication with the USR. In one embodiment, the USR element 768 authenticates the user based on the value that is communicated from the device 735. Successful authentication allows the user of the device 735 to unlock the computer to access local or remote resources. The resources can include any of files, images, forms, e-mail,

- 61 -

document management systems, catalogs or other information whether located locally on the computer 736 or accessible over a network such as the Internet or an intranet. Thereafter, the device 735 and the computer 736 can periodically communicate where the device 735 communicates subsequent time-varying non-predictable values to the computer for ongoing authentication. According to this embodiment, the computer remains operable to the user (for example, unlocked) so long as the computer continues to receive subsequent authentication values. In accordance with one embodiment, the subsequent authentication values also include a time-varying non-predictable value.

In one embodiment, the initial time-varying non-predictable value used to authenticate the user and unlock the computer includes only a portion of a larger time-varying non-predictable value. In this example, subsequent time-varying non-predictable values can include additional portions of the same time-varying non-predictable value, or a portion of or all of a newly-generated time-varying non-predictable value. In alternate embodiments, a complete time-varying non-predictable value (for example, a 20+ character value with the full set of characters as generated) is employed for the initial authentication and newly-generated time-varying non-predictable values are employed for each of the subsequent authentications, respectively, to maintain the computer 736 in an unlocked state. Depending upon the embodiment, these subsequent authentications can employ a time-varying non-predictable value including a 20+ character value with the full set of characters as generated or a time-varying non-predictable value that includes a subset of the full set of characters. According to some embodiments, the time-varying non-predictable value only includes numeric characters and the subset is a subset of digits. According to other embodiments, the time-varying non-predictable value includes both alpha and numeric characters (for example, a value represented in hexadecimal notation).

In one embodiment, static identifying information is not included and the system 730 employs an identification process as described elsewhere herein. In accordance with an alternate embodiment, at least some form of static identifying information concerning the user is communicated with the non-predictable value in a verification process that is employed

- 62 -

either locally at the computer 736, with the USR element 768, or remotely at the USR 734 to authenticate the user.

As mentioned above, the system 730 can maintain the computer 736 in the unlocked state so long as time-varying non-predictable values are received subsequent to the initial authentication, and provided that these later received values are successfully authenticated.
5 Thus, where the user moves with the wireless user device out of the proximity of the computer (for example, out of wireless range) the computer 736 can go into a locked state that will prevent its further use until an authentication protocol is successfully initiated by the same or a different user.

10 In some embodiments, the system 730 employs an initial user authentication process such as the process 580 described in association with embodiments of FIG. 10, for example, a “handshake” or bilateral authentication must be completed at a start of the process to unlock the computer. However, in one embodiment, the computer can temporarily lock-up for a permissible time period following the initial successful user authentication. Provided that the
15 user returns within the permissible time-period, the computer will unlock (provided that a subsequent time-varying non-predictable values is received and successfully authenticated) without need for the user to repeat the initial user authentication process.

In this example, the computer 736 is unlocked with an initial authentication and remains in the unlocked state so long as the subsequent time-varying non-predictable values is
20 received and successfully authenticated. Where a subsequent time-varying non-predictable value is received and not successfully authenticated, the computer 736 will return to a locked state that requires a user to complete the initial user authentication process to unlock the computer 734. However, where the computer stops receiving subsequent time-varying non-predictable values for less than a predetermined period of time (for example, a matter of
25 minutes when the user has momentarily left the immediate vicinity of the computer) that user can return and unlock the computer with the successful authentication of subsequent time-varying non-predictable values generated with the wireless user device without beginning the authentication process anew.

- 63 -

The computer 736 can be configured to authenticate one or more users to employ one or more wireless user devices 735. For example, computer 736 can be accessible to a plurality of users where each of the users employs a different wireless device 735, respectively.

According to these embodiments, the computer can maintain (or access via USR 734)

5 authentication information such as seeds for each of the plurality of authorized users. Further, each of the plurality of wireless user devices generates time-varying non-predictable values independently of others of the plurality of wireless user devices.

Further, activation of the wireless user device 735 can employ approaches described herein using multiple factors including something the user knows, something the user has,

10 something the user is alone or in combination with each other or with additional factors. Thus, in accordance with one embodiment the wireless user device 735 includes a seed that is used to generate a time-varying non-predictable value. In accordance with some embodiments, the seed 757 is provided by the USR 734 in the manner described else where herein. In

accordance with a further embodiment, the electronic serial number of the wireless user device

15 735 can also be employed as a seed either alone or in combination with the USR seed 757.

Similarly, the subscriber identity module can include information that is employed alone or in combination with the USR seed 757 and/or the electronic serial number 759 as a seed that is used to generate a time-varying non-predictable value. As should be apparent, the approach

then employs the seed to generate the time-varying non-predictable value and also employs a

20 temporal element such as the current time, for example, a time at which the code or the value is generated. According to some embodiments, the processor of the wireless user device 735 is

configured to employ time, secret information known to the user and a seed to generate the

time-varying non-predictable value. In accordance with further embodiments the processor is configured to generate the non-predictable value at least in part by combining the secret

25 information and the seed and in an exclusive-or operation. Either or both of the electronic

serial number 759 and the SIM number 758 may be employed in any combination with the

preceding to further increase security of the multi-factor authentication process.

- 64 -

According to some embodiments, the subsequent time-varying non-predictable values are generated for subsequent time periods, respectively. The selection of the increment of time that provides the subsequent time periods can be selected based on the embodiment such that a new period of time occurs with a relatively high frequency in high security applications or at a lower frequency for lower security applications. Accordingly, depending upon the embodiment, the subsequent time-varying non-predictable value used in an authentication process can refer to a time-varying non-predictable value that is generated for a time period that is immediately subsequent to the preceding time-period or a later occurring time-period. For example, the NPV #1, the NPV #2 and the NPV #3 can be generated for three consecutive time periods or in sequence for time periods that include one or more time periods for which a NPV is not generated and transmitted. The approach can vary depending upon a length established for the time periods and the time required for a transmission and/or processing of the time-varying non-predictable value. In one embodiment, the USR system operates to vary the length of the time periods to increase security.

The preceding embodiments can be employed to provide an uncounterfeitable token that may be used in processes that have increased security relative to prior approaches.

According to some embodiments, an electronic wallet included in a mobile phone allows one to use any number of credit or debit cards at the point-of-sale where no private, sensitive, or secret information or account numbers are stored in the device or transmitted by near field communication ("NFC"). In further embodiments, the electronic wallet, in addition to NFC, can also communicate in Bluetooth and Wi-Fi and can be used for interpersonal funds transfer, computer network access, access to physical facilities and to otherwise authenticate one's identity and act as an individual's trusted agent.

In some embodiments, a user must satisfy 3 factor security to make a transaction, for example, by using a discreet token (the mobile phone), a secret (the users PIN), and a voice print (a biometric). In these embodiments, the biometric can not be recorded and replayed because the biometric required for authentication and/or device activation is a new code that must be spoken digit-by-digit with each authentication. In embodiments where a digital

- 65 -

picture of the identified user is sent to POS from USR the requirements of; 3+ factor security™ are met.

Embodiments of the system and method described herein can employ identification technology to increase security because no static abusable or exploitable static identifier is used. The preceding feature distinguishes these embodiments from verification technology
5 where some form of static identifier is required. Further, where static identifying information is not employed, the generated, successful, unpredictable code transmitted from the mobile user device represents satisfaction of all three security factors and identifies, rather than verifies, the identification of the user.

10 Further, the various embodiments described herein can be employed in an identification process or a verification process depending on the specific embodiment. For example, in one approach (identification) static identifying information that identifies the user is not included with the transmitted random one-time code. Because an identification process provides increased security, in this embodiment, the USR employs a code matching algorithm to
15 authenticate the user's identity without benefit of any static identifying information. In contrast, in another approach for the embodiments described herein the USR employs the static identifying information in combination with a code matching algorithm to authenticate the user's identity.

In some embodiments, no PIN is stored in the token. In some of these embodiments, the
20 PIN is integrated with the algorithm and never stored, transmitted, or exposed.

In the improbable circumstance where at a particular time period more than one unpredictable code is generated for more than one user at USR, USR can in some embodiments wait for the next (immediately subsequent in time) code to authenticate based on a user's unique identity.

25 Further, in some embodiments, a "token" can first send a non-transactional subset non-predictable code to the USR server. The server then sends a subset of the next code that the USR token would generate to the token. Thus, the server has demonstrated its authenticity to the token and then the token can send the actual, active, non-predictable code to the now

- 66 -

trusted, authenticated secure USR server.

Still further, in various embodiments, some of the preceding can employ, or be employed in, apparatus, systems and methods where a verification process is used. For example, the non-predictable value can be communicated along with static identifying information. Where even greater security is required an identification process can be employed. For example, with the identification process, the non-predictable value can be communicated without any static identifying information.

According to any of the preceding embodiments, the mobile devices each include a GPS. According to these embodiments, the GPS capabilities can be used to track user activities and apply security criteria that can act to limit transaction activity based on the location of the mobile device and/or the relative change in position of the mobile device.

According to each of the preceding embodiments in which a PIN is employed to generate a non-predictable value communicated for authentication, the PIN need not be stored in the wireless user-device. According to these embodiments, the PIN can be supplied by the user and immediately employed in an algorithm used to generate the non-predictable value (for example, a time-varying non-predictable value).

It should also be appreciated that any of the apparatus, systems and methods described herein can be used with, or in the manner described in U.S. Patent Nos. 7,237,117; 7,809,651; 7,805,372; 8,001,055; and U.S. Patent Application No. 12/393,586 each of which is herein incorporated by reference in its entirety for all purposes. For example, in various embodiments, the systems 650 and 730 disclosed herein can operate in the manner of any one of the systems described in the previously-identified U.S. Patents and Application and provide any of the functionality of the systems described therein. Similarly, in various embodiments, the USRs 10, 640, 654 and 734 disclosed herein can operate in the manner of any one of the secure registries described in the previously-identified U.S. Patents and Applications and provide the functionality of any of the secure registries described therein. Further, the wireless user devices and/or tokens 674, 652 and 734 can take the form of any one of the user devices

- 67 -

and/or tokens that are described in the previously-identified U.S. Patents and Applications and provide the functionality of any of the user devices and/or tokens described therein.

As used herein, the terms “wireless device” and “wireless user device” describe apparatus that can wirelessly communicate. These terms encompass devices that can include
5 both wireless communication and wired communication depending upon the manner in which the apparatus is used. For example, as used herein, a “wireless device” can include a USB or other hardwired communication port for temporary or permanent connection to another device and/or network. As will be apparent, a “wireless device” can also include a port for connection to a power source for operating power and/or battery recharging. Further, the embodiments of
10 the wireless user devices described herein can each include a clock (such as an oscillator) used as a time-reference. In some embodiments, the clock is a discrete element while in other embodiments the clock can be included in another element, for example, a microcontroller of the wireless user device. Wireless user devices can also include any of electronic ID devices, mobile phones, PDAs, personal computers, fobs, wristwatches, passports, pens, credit cards
15 and dongles as some examples.

Having thus described several aspects of at least one embodiment of this invention, it is to be appreciated various alterations, modifications, and improvements will readily occur to those skilled in the art. Such alterations, modifications, and improvements are intended to be part of this disclosure, and are intended to be within the spirit and scope of the invention.
20 Accordingly, the foregoing description and drawings are by way of example only.

What is claimed is:

- 68 -

CLAIMS

1. A system for controlling access to at least one computer, the system comprising:
a network having at least a portion that includes a wireless network;
5 at least one computer coupled to the network;
a handheld device configured to communicate with the at least one computer over the
wireless network, the handheld device including:
a user interface programmed to receive a user input including secret information
known to a user of the handheld device;
10 a processor coupled to the user interface, the processor programmed to
authenticate the user of the handheld device and to generate a first time-varying non-
predictable value following a successful authentication, by the handheld device, of the
secret information received via the user interface; and
a wireless transceiver coupled to the processor and configured to transmit via
15 the network a wireless signal including the first time-varying non-predictable value;
and
a secure registry system including a communication interface coupled to the network,
the secure registry system configured to receive the first time-varying non-predictable value
and successfully authenticate the user where the first time-varying non-predictable value is
20 matched to the user by the secure registry system,
wherein the user of the handheld device is permitted to operate the at least one
computer to access resources with the at least one computer so long as the at least one
computer periodically receives subsequent authentication information from the handheld
device that results in a continued successful authentication of the user for time periods
25 subsequent to a time at which the first time-varying non-predictable value is generated.

- 69 -

2. The system of claim 1, wherein the secure registry system is configured to lock the computer to prevent the user from operating the computer to access resources when the computer fails to periodically receive the subsequent authentication information.
- 5 3. The system of claim 2, wherein the secure registry system is configured to lock the computer to prevent the user from operating the computer to access resources when the computer fails to periodically receive the subsequent authentication information because the handheld device is no longer within proximity of the computer.
- 10 4. The system of claim 3, wherein the wireless network includes any one of a Wi-fi communication, near field communication and Bluetooth communication employed for communication between the computer and the handheld device, and
wherein the proximity is determined by a range of the wireless network local to the computer.
- 15 5. The system of claim 4, wherein the handheld device includes any of a mobile phone, a tablet computer and a personal digital assistant, and
wherein the computer includes any one of a desktop computer, a notebook computer, a laptop computer, a netbook computer and a tablet computer.
- 20 6. The system of claim 3, wherein the secure registry system is coupled to a plurality of computers, the computers each associated with a plurality of users, respectively, and
wherein the secure registry system is configured to authenticate each of the plurality of users to provide access for each user to at least one computer associated with the user,
25 respectively.
7. The system of claim 6, wherein the plurality of users includes a second user associated with a second computer,

- 70 -

wherein the second user is in possession of a second handheld device including a second processor, and

wherein the processor is configured to generate a second time-varying non-predictable value following a successful authentication of the second user by the second device.

5

8. The system of claim 7, wherein the second handheld device includes a second wireless transceiver coupled to the second processor and configured to transmit via a second network a second wireless signal including the second time-varying value,

wherein the communication interface of the secure registry is configured to receive the second time-varying non-predictable value and successfully authenticate the second user where the second time-varying non-predictable value is matched to the second user by the secure registry system, and

wherein the second user is permitted to operate the second computer to access resources so long as subsequent authentication information from the second handheld device of the second user results in a continued successful authentication of the second user for time periods subsequent to a time at which the second time-varying non-predictable value is generated.

9. The system of claim 8, wherein the secure registry is configured to lock the first computer to prevent access to resources using the first computer when the first computer fails to periodically receive authentication information subsequent to the time at which the first time-varying non-predictable value is generated because the first handheld device is no longer within proximity of the first computer, and

wherein the secure registry is configured to lock the second computer to prevent access to resources using the second computer when the second computer fails to periodically receive authentication information subsequent to the time at which the second time-varying non-predictable value is generated because the second handheld device is no longer within proximity of the second computer.

- 71 -

10. The system of claim 1, wherein the secure registry system is located remote from the computer, and
wherein the authentication of the first time-varying non-predictable value and any
5 subsequent time-varying non-predictable values occur at the secure registry system.
11. The system of claim 1, wherein at least a portion of the secure registry system is located at the computer, and
wherein the authentication of the first time-varying non-predictable value and any
10 subsequent time-varying non-predictable values occur at the computer.
12. The system of claim 1, wherein the handheld device includes a memory coupled to the processor, the memory configured to store a seed employed by the processor to generate the first time-varying non-predictable value; and
15 wherein the processor is configured to employ time, the secret information and the seed to generate the first time-varying non-predictable value.
13. The system of claim 12, wherein the secure registry is configured to distribute seed-updates to the handheld device via the network without requiring any interaction on the part of
20 the user, and
wherein the seed-updates are communicated at random intervals to provide a new seed value to the handheld device.
14. The system of claim 13, wherein at least a portion of the secure registry system is
25 located in a computer, the computer proximate the handheld device when the wireless signal is transmitted,
wherein the computer includes a memory configured to store the seed, and
wherein the seed is employed by the computer to authenticate the user.

- 72 -

15. The system of claim 14, wherein the processor is configured to combine the secret information with the seed to generate the first time-varying non-predictable value.
- 5 16. The system of claim 15, wherein the processor is configured to generate the first time-varying non-predictable value, at least in part, by combining the secret information and the seed in an exclusive-or operation, and
wherein the secret information is not stored in the handheld device.
- 10 17. The system of claim 14, wherein the memory is configured to store at least one of an electronic serial number and a SIM code, and
wherein the processor is configured to generate the first time-varying non-predictable value, at least in part, by combining the seed with at least one of the electronic serial number and the SIM code in an exclusive-or operation.
- 15 18. The system of claim 17, wherein the secret information is not stored in the handheld device.
19. The system of claim 17, wherein the handheld device includes a secure element, and
20 wherein the secure element is configured to store at least one of the seed and the electronic serial number.
20. The system of claim 14, wherein the handheld device includes a biometric sensor comprising a microphone configured to receive a spoken input provided by the user,
25 wherein the user interface is programmed to display a multi-character string including at least one of a plurality of alpha-characters and a plurality of numeric-characters, and
wherein the processor is programmed to authenticate the user based on the spoken input of the multi-character string by the user.

- 73 -

21. The system of claim 21, wherein the secure registry system is programmed to randomly generate the multi-character string and communicate the multi-character string via the network to the handheld device for display,
- 5 wherein at least a portion of the secure registry system is located in a computer, the computer proximate the handheld device when the wireless signal is transmitted, and wherein the at least the portion of the secure registry located in the computer is configured to generate the multi-character string.
- 10 22. The system of claim 11, wherein the secure registry system includes a database configured to store the seed, wherein, following a successful authentication of the user, the secure registry system is configured to generate a second time-varying non-predictable value using time, the secret information and the seed,
- 15 wherein the communication interface is configured to transmit the second time-varying non-predictable value to the handheld device via the network, and wherein the processor is configured to authenticate the secure registry system using the second time-varying non-predictable value.
- 20 23. The system of claim 22, wherein the processor is configured to, following a successful authentication of the secure registry system, generate a third time-varying non-predictable value, wherein the wireless signal is a first wireless signal, wherein the wireless transceiver is configured to transmit via the network a second
- 25 wireless signal including the third time-varying non-predictable value, and wherein the secure registry system is configured to authenticate the user using the third time-varying non-predictable signal.

- 74 -

24. A method of securing a computing device, the method comprising:
receiving, at the computing device, a first wireless signal including first authentication information wirelessly transmitted from a mobile device proximate to the computing device;
processing the first authentication information to initially authenticate a user in
5 possession of the mobile device, the user attempting to access resources with the computing device;
temporarily allowing the user to employ the computing device to access the resources when the initial authentication is successful;
continuing to allow the user to employ the computing device to access the resources
10 upon a subsequent receipt of authentication information from the mobile device that is successfully authenticated; and
automatically terminating use of the computing device by the user based on at least one of authentication information no longer being received from the mobile device and authentication information received from the mobile device no longer being successfully
15 authenticated.
25. The method of securing a computing device of claim 24, further comprising:
receiving, at the computing device, subsequent wireless signals from the first wireless device on a periodic basis, the periodic basis including a predetermined period during which
20 the computing device must receive authentication information;
continuing to allow the user to employ the computing device to access the resources where the subsequent wireless signals include authentication information that is successfully authenticated; and
terminating use of the computing device when at least one of the subsequent wireless
25 signals is not received during a respective predetermined period.

- 75 -

26. The method of claim 24, further comprising:
including at least a first time-varying non-predictable value generated by the mobile device in the first authentication information; and
including in the authentication information included in each of the subsequent wireless
5 signals a respective time-varying non-predictable value generated by the mobile device.
27. The method of claim 26, further comprising initially authenticating the user of the mobile device when the first time-varying non-predictable value is matched to the user by a secure registry system geographically remote from the computing device.
10
28. The method of claim 27, further comprising subsequently authenticating the user of the mobile device at each occurrence where the respective time-varying non-predictable value is matched to the user by the secure registry.
- 15 29. The method of claim 27, further comprising:
including at least a portion of the secure registry system in the computing device; and
locally authenticating the user with the computing device.
30. The method of claim 29, further comprising:
20 including public identifying information of the user in the authentication information;
and
authenticating the user by comparing the time-varying non-predictable value received in the wireless signal with verification information for the user based on an identity provided by the public identifying information.
25
31. The method of claim 24, further comprising:
locating at least a portion of the secure registry system remote from the computing device;

- 76 -

communicating the first time-varying non-predictable value to the remote portion of the secure registry system for an initial authentication; and

locally authenticating the respective time-varying non-predictable values with the computing device.

5

32. The method of claim 25, further comprising maintaining an ability for the mobile device to wirelessly communicate with the computing device so long as the mobile device is located within a pre-determined distance of the computing device.

10 33. The method of claim 24, wherein the mobile device includes any of a personal digital assistant, mobile phone and a tablet computer, and

wherein the method further comprises communicating the wireless signal by one of Bluetooth, near field communication and Wi-Fi.

AMENDED CLAIMS
received by the International Bureau on 20 March 2012 (20.03.2012)

1. A system for controlling access to at least one computer, the system comprising:
 - a network having at least a portion that includes a wireless network;
 - at least one computer coupled to the network;
 - a handheld device configured to communicate with the at least one computer over the wireless network, the handheld device including:
 - a user interface programmed to receive a user input including secret information known to a user of the handheld device;
 - a processor coupled to the user interface, the processor programmed to authenticate the user of the handheld device and to generate a first time-varying non-predictable value following a successful authentication, by the handheld device, of the secret information received via the user interface; and
 - a wireless transceiver coupled to the processor and configured to transmit via the network a wireless signal including the first time-varying non-predictable value; and
 - a secure registry system including a communication interface coupled to the network, the secure registry system configured to receive the first time-varying non-predictable value and successfully authenticate the user where the first time-varying non-predictable value is matched to the user by the secure registry system,
- wherein the user of the handheld device is permitted to operate the at least one computer to access resources with the at least one computer so long as the at least one computer periodically receives subsequent authentication information from the handheld device that results in a continued successful authentication of the user for time periods subsequent to a time at which the first time-varying non-predictable value is generated.

2. The system of claim 1, wherein the secure registry system is configured to lock the computer to prevent the user from operating the computer to access resources when the computer fails to periodically receive the subsequent authentication information.
3. The system of claim 2, wherein the secure registry system is configured to lock the computer to prevent the user from operating the computer to access resources when the computer fails to periodically receive the subsequent authentication information because the handheld device is no longer within proximity of the computer.
4. The system of claim 3, wherein the wireless network includes any one of a Wi-fi communication, near field communication and Bluetooth communication employed for communication between the computer and the handheld device, and
wherein the proximity is determined by a range of the wireless network local to the computer.
5. The system of claim 4, wherein the handheld device includes any of a mobile phone, a tablet computer and a personal digital assistant, and
wherein the computer includes any one of a desktop computer, a notebook computer, a laptop computer, a netbook computer and a tablet computer.
6. The system of claim 3, wherein the secure registry system is coupled to a plurality of computers, the computers each associated with a plurality of users, respectively, and
wherein the secure registry system is configured to authenticate each of the plurality of users to provide access for each user to at least one computer associated with the user, respectively.

7. The system of claim 6, wherein the plurality of users includes a second user associated with a second computer,
wherein the second user is in possession of a second handheld device including a second processor, and
wherein the processor is configured to generate a second time-varying non-predictable value following a successful authentication of the second user by the second device.
8. The system of claim 7, wherein the second handheld device includes a second wireless transceiver coupled to the second processor and configured to transmit via a second network a second wireless signal including the second time-varying value,
wherein the communication interface of the secure registry is configured to receive the second time-varying non-predictable value and successfully authenticate the second user where the second time-varying non-predictable value is matched to the second user by the secure registry system, and
wherein the second user is permitted to operate the second computer to access resources so long as subsequent authentication information from the second handheld device of the second user results in a continued successful authentication of the second user for time periods subsequent to a time at which the second time-varying non-predictable value is generated.
9. The system of claim 8, wherein the secure registry is configured to lock the first computer to prevent access to resources using the first computer when the first computer fails to periodically receive authentication information subsequent to the time at which the first time-varying non-predictable value is generated because the first handheld device is no longer within proximity of the first computer, and
wherein the secure registry is configured to lock the second computer to prevent access to resources using the second computer when the second computer fails to periodically receive authentication information subsequent to the time at which the second time-varying non-

predictable value is generated because the second handheld device is no longer within proximity of the second computer.

10. The system of claim 1, wherein the secure registry system is located remote from the computer, and

wherein the authentication of the first time-varying non-predictable value and any subsequent time-varying non-predictable values occur at the secure registry system.

11. The system of claim 1, wherein at least a portion of the secure registry system is located at the computer, and

wherein the authentication of the first time-varying non-predictable value and any subsequent time-varying non-predictable values occur at the computer.

12. The system of claim 1, wherein the handheld device includes a memory coupled to the processor, the memory configured to store a seed employed by the processor to generate the first time-varying non-predictable value; and

wherein the processor is configured to employ time, the secret information and the seed to generate the first time-varying non-predictable value.

13. The system of claim 12, wherein the secure registry is configured to distribute seed-updates to the handheld device via the network without requiring any interaction on the part of the user, and

wherein the seed-updates are communicated at random intervals to provide a new seed value to the handheld device.

14. The system of claim 13, wherein at least a portion of the secure registry system is located in a computer, the computer proximate the handheld device when the wireless signal is transmitted,
wherein the computer includes a memory configured to store the seed, and
wherein the seed is employed by the computer to authenticate the user.
15. The system of claim 14, wherein the processor is configured to combine the secret information with the seed to generate the first time-varying non-predictable value.
16. The system of claim 15, wherein the processor is configured to generate the first time-varying non-predictable value, at least in part, by combining the secret information and the seed in an exclusive-or operation, and
wherein the secret information is not stored in the handheld device.
17. The system of claim 14, wherein the memory is configured to store at least one of an electronic serial number and a SIM code, and
wherein the processor is configured to generate the first time-varying non-predictable value, at least in part, by combining the seed with at least one of the electronic serial number and the SIM code in an exclusive-or operation.
18. The system of claim 17, wherein the secret information is not stored in the handheld device.
19. The system of claim 17, wherein the handheld device includes a secure element, and
wherein the secure element is configured to store at least one of the seed and the electronic serial number.

20. The system of claim 14, wherein the handheld device includes a biometric sensor comprising a microphone configured to receive a spoken input provided by the user,
wherein the user interface is programmed to display a multi-character string including at least one of a plurality of alpha-characters and a plurality of numeric-characters, and
wherein the processor is programmed to authenticate the user based on the spoken input of the multi-character string by the user.
21. The system of claim 20, wherein the secure registry system is programmed to randomly generate the multi-character string and communicate the multi-character string via the network to the handheld device for display,
wherein at least a portion of the secure registry system is located in a computer, the computer proximate the handheld device when the wireless signal is transmitted, and
wherein the at least the portion of the secure registry located in the computer is configured to generate the multi-character string.
22. The system of claim 11, wherein the secure registry system includes a database configured to store the seed,
wherein, following a successful authentication of the user, the secure registry system is configured to generate a second time-varying non-predictable value using time, the secret information and the seed,
wherein the communication interface is configured to transmit the second time-varying non-predictable value to the handheld device via the network, and
wherein the processor is configured to authenticate the secure registry system using the second time-varying non-predictable value.
23. The system of claim 22, wherein the processor is configured to, following a successful authentication of the secure registry system, generate a third time-varying non-predictable value,

wherein the wireless signal is a first wireless signal,
wherein the wireless transceiver is configured to transmit via the network a second wireless signal including the third time-varying non-predictable value, and
wherein the secure registry system is configured to authenticate the user using the third time-varying non-predictable signal.

24. A method of securing a computing device, the method comprising:
receiving, at the computing device, a first wireless signal including first authentication information wirelessly transmitted from a mobile device proximate to the computing device;
processing the first authentication information to initially authenticate a user in possession of the mobile device, the user attempting to access resources with the computing device;
temporarily allowing the user to employ the computing device to access the resources when the initial authentication is successful;
continuing to allow the user to employ the computing device to access the resources upon a subsequent receipt of authentication information from the mobile device that is successfully authenticated; and
automatically terminating use of the computing device by the user based on at least one of authentication information no longer being received from the mobile device and authentication information received from the mobile device no longer being successfully authenticated.

25. The method of securing a computing device of claim 24, further comprising:
receiving, at the computing device, subsequent wireless signals from the first wireless device on a periodic basis, the periodic basis including a predetermined period during which the computing device must receive authentication information;
continuing to allow the user to employ the computing device to access the resources where the subsequent wireless signals include authentication information that is successfully authenticated; and

terminating use of the computing device when at least one of the subsequent wireless signals is not received during a respective predetermined period.

26. The method of claim 24, further comprising:
including at least a first time-varying non-predictable value generated by the mobile device in the first authentication information; and
including in the authentication information included in each of the subsequent wireless signals a respective time-varying non-predictable value generated by the mobile device.
27. The method of claim 26, further comprising initially authenticating the user of the mobile device when the first time-varying non-predictable value is matched to the user by a secure registry system geographically remote from the computing device.
28. The method of claim 27, further comprising subsequently authenticating the user of the mobile device at each occurrence where the respective time-varying non-predictable value is matched to the user by the secure registry.
29. The method of claim 27, further comprising:
including at least a portion of the secure registry system in the computing device; and
locally authenticating the user with the computing device.
30. The method of claim 29, further comprising:
including public identifying information of the user in the authentication information; and
authenticating the user by comparing the time-varying non-predictable value received in the wireless signal with verification information for the user based on an identity provided by the public identifying information.

31. The method of claim 24, further comprising:
locating at least a portion of the secure registry system remote from the computing device;
communicating the first time-varying non-predictable value to the remote portion of the secure registry system for an initial authentication; and
locally authenticating the respective time-varying non-predictable values with the computing device.
32. The method of claim 25, further comprising maintaining an ability for the mobile device to wirelessly communicate with the computing device so long as the mobile device is located within a pre-determined distance of the computing device.
33. The method of claim 24, wherein the mobile device includes any of a personal digital assistant, mobile phone and a tablet computer, and
wherein the method further comprises communicating the wireless signal by one of Bluetooth, near field communication and Wi-Fi.

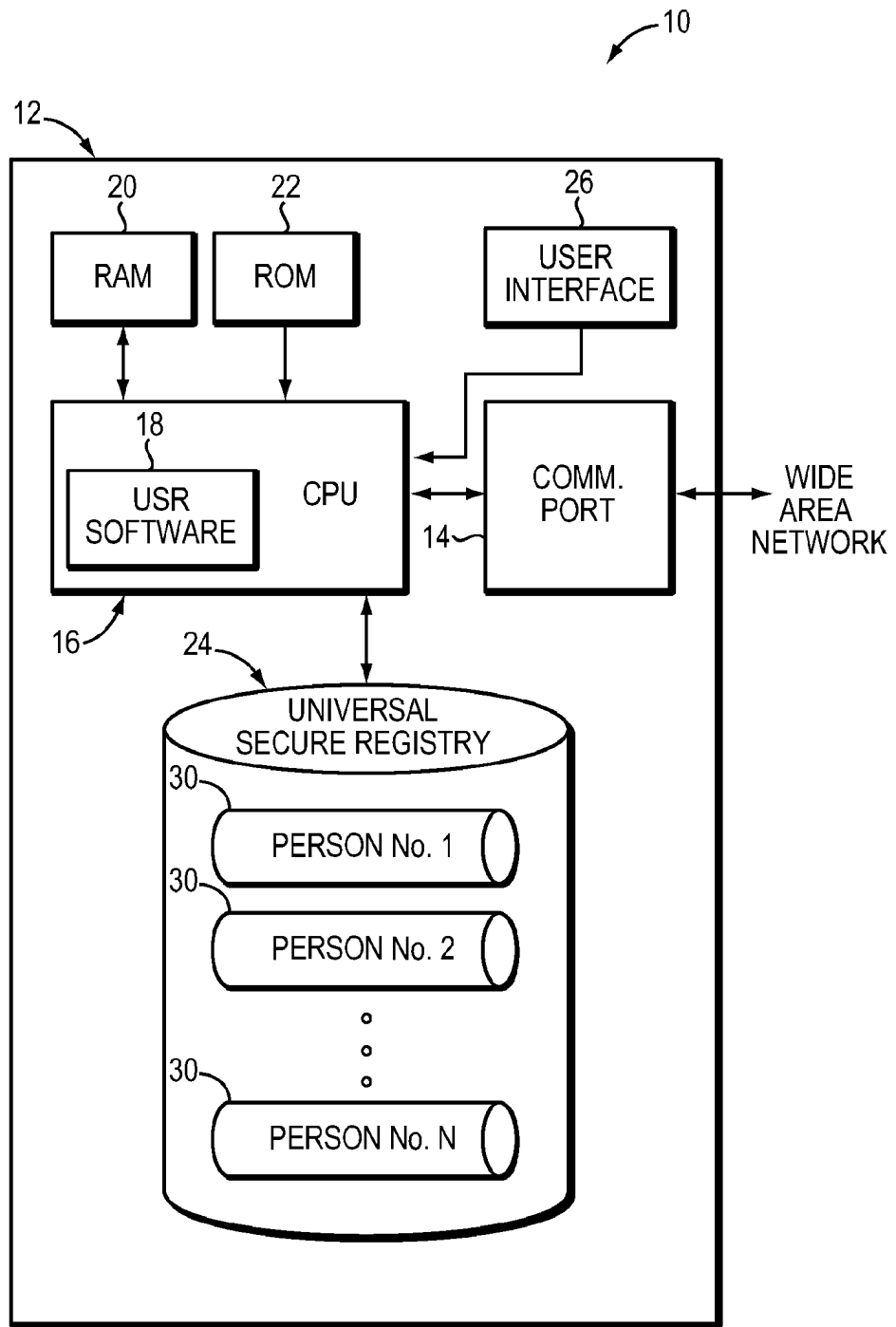


FIG. 1



+

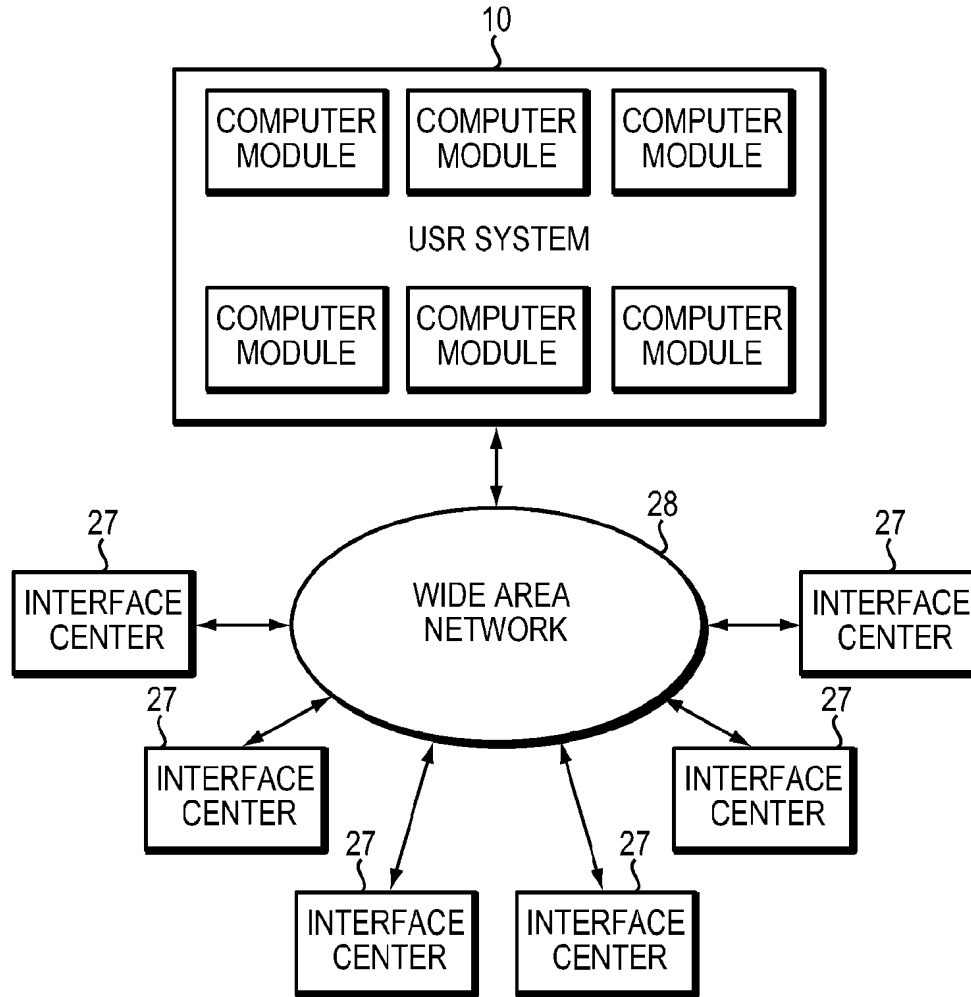


FIG. 2

+

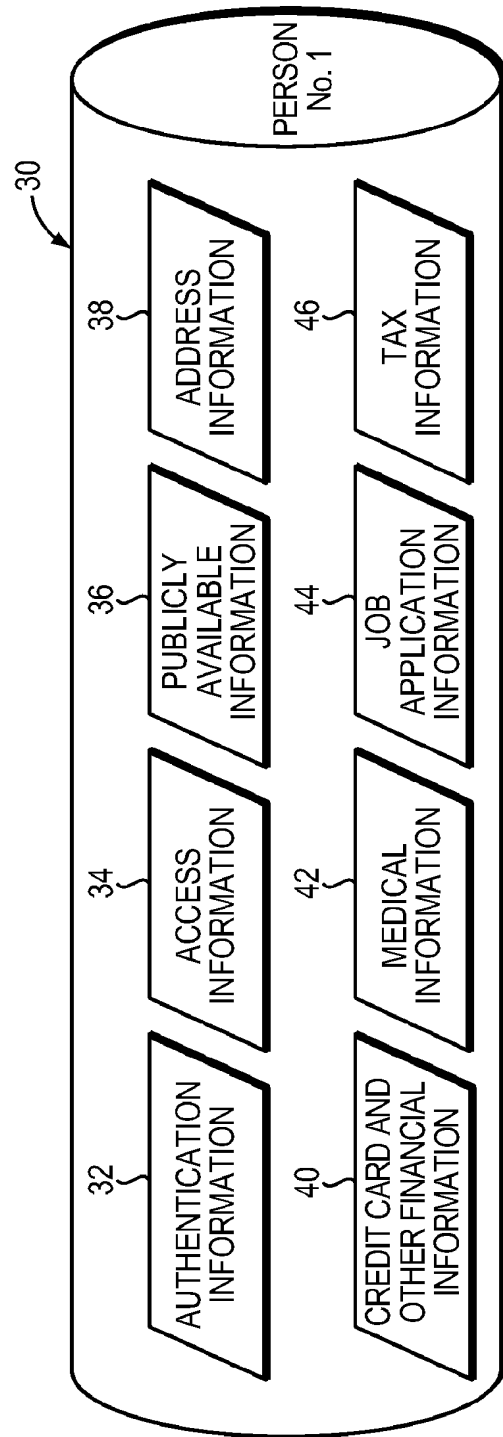


FIG. 3





4/12

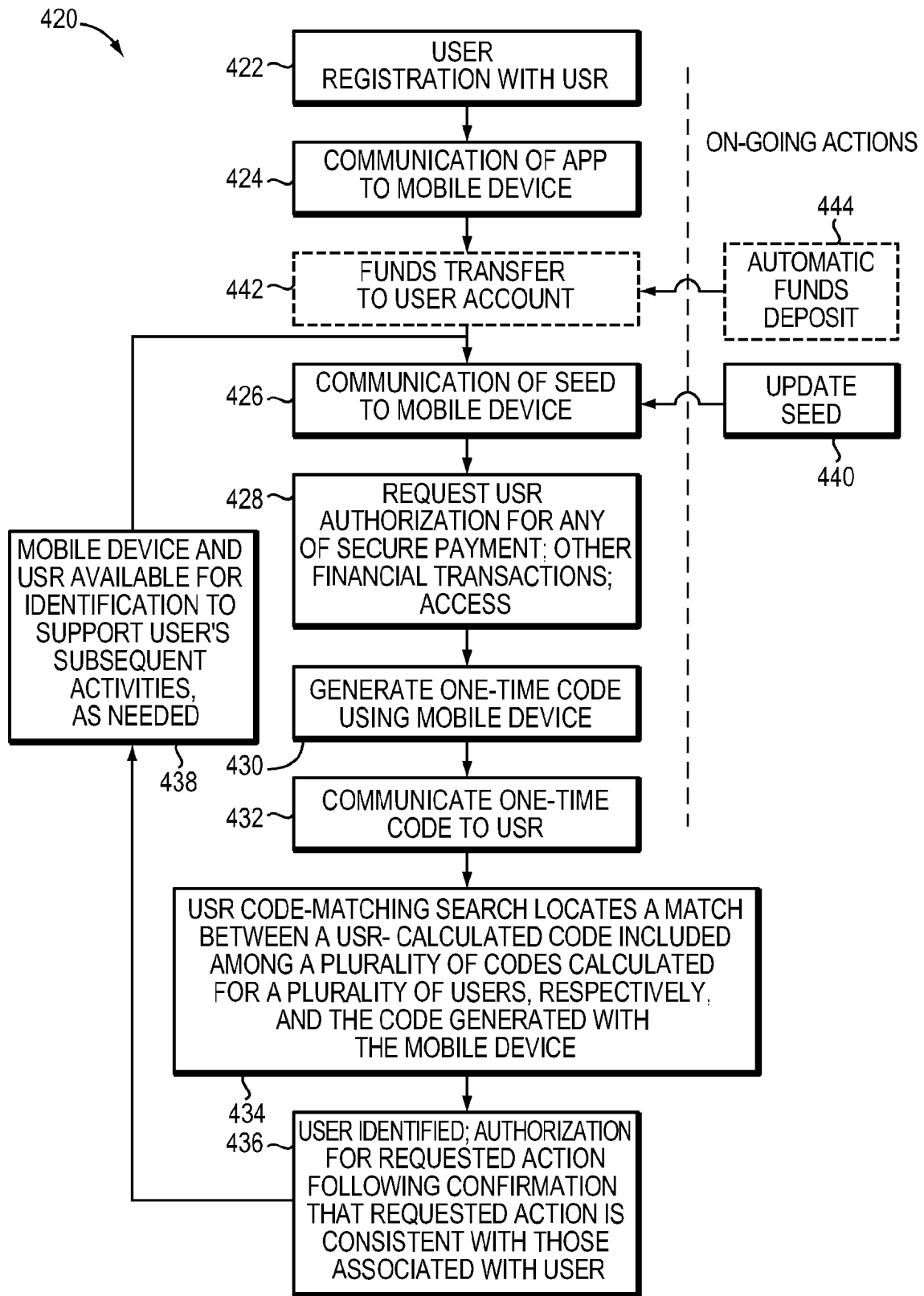


FIG. 4





5/12

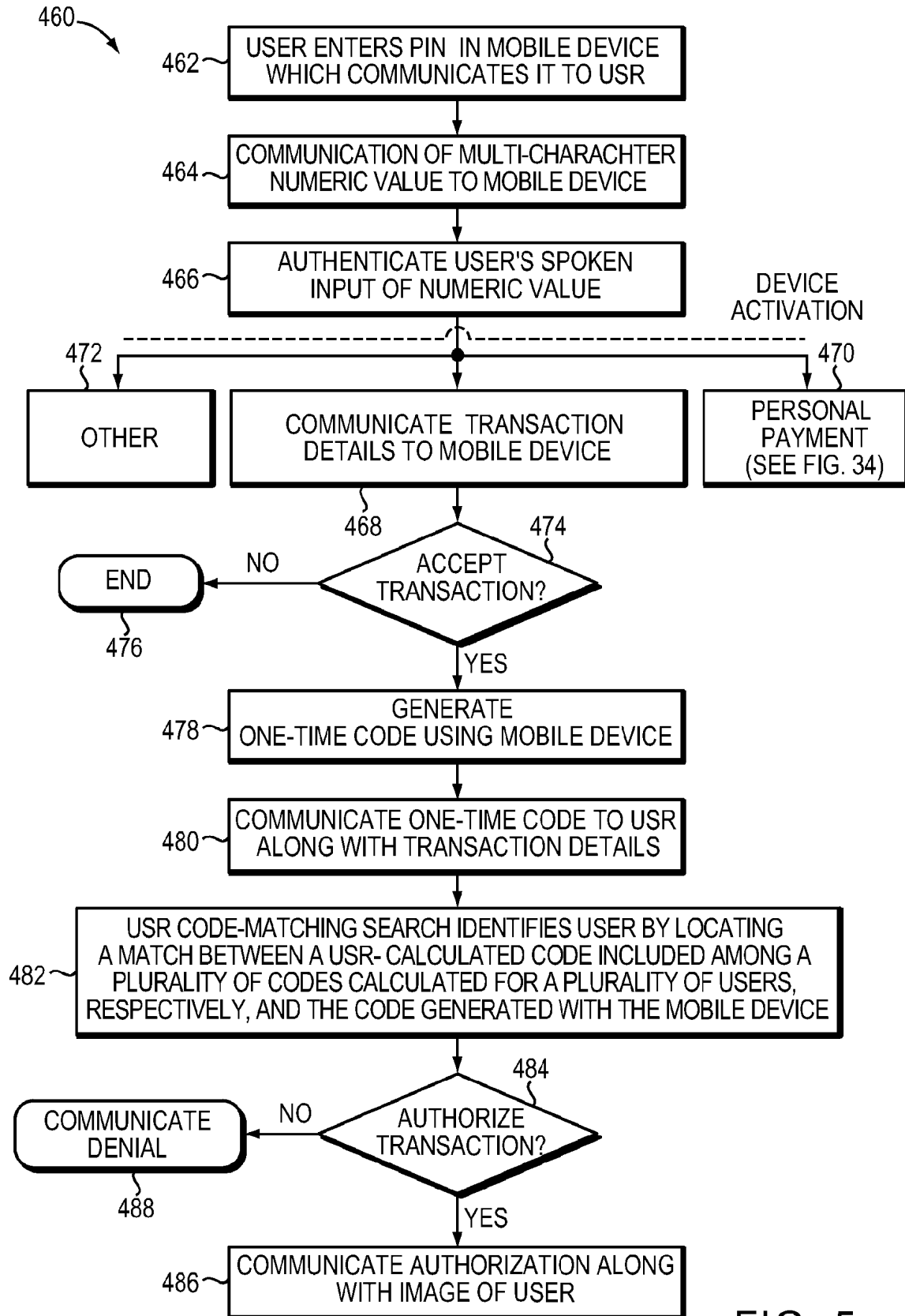


FIG. 5



6/12

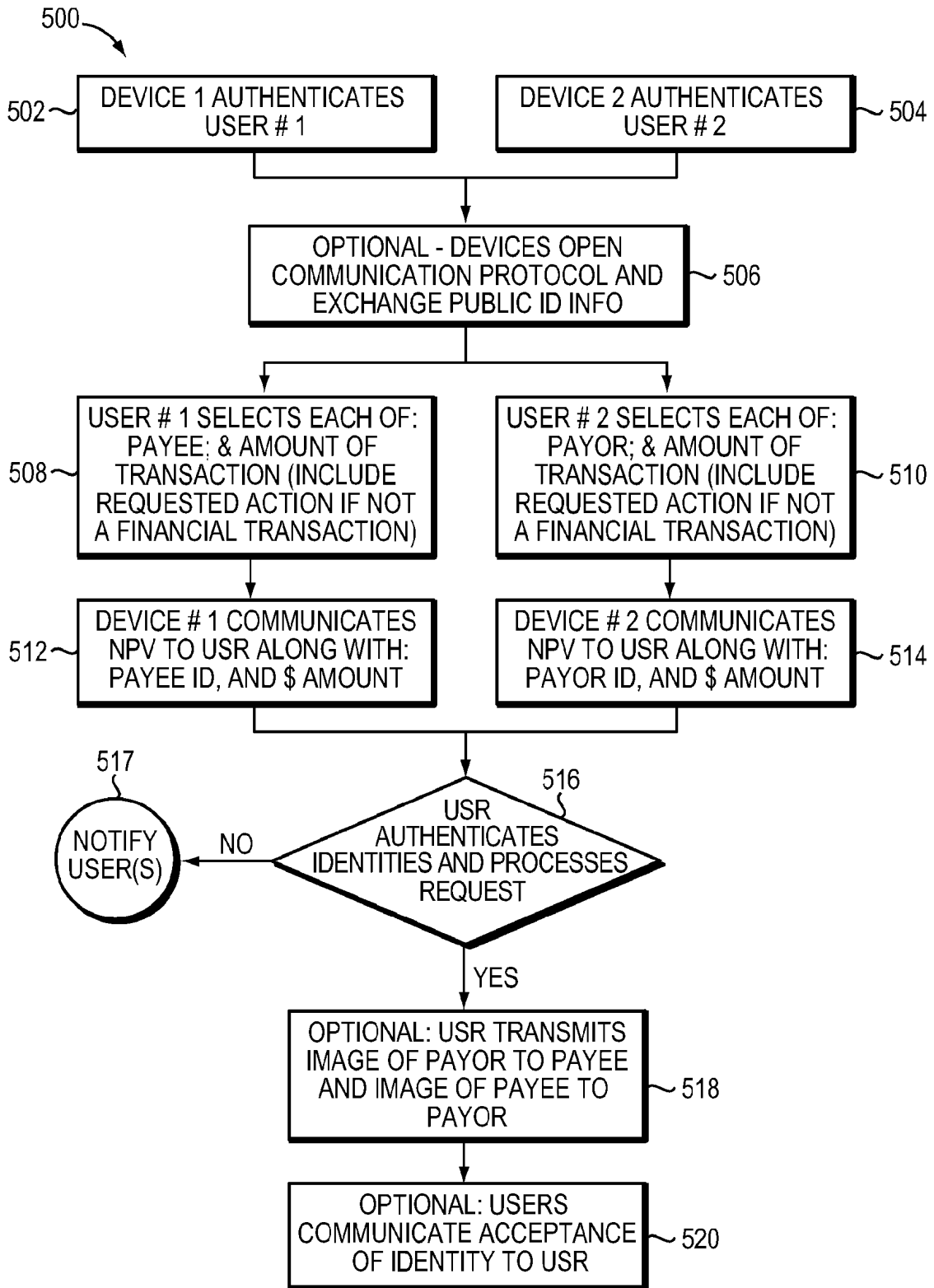


FIG. 6



7/12

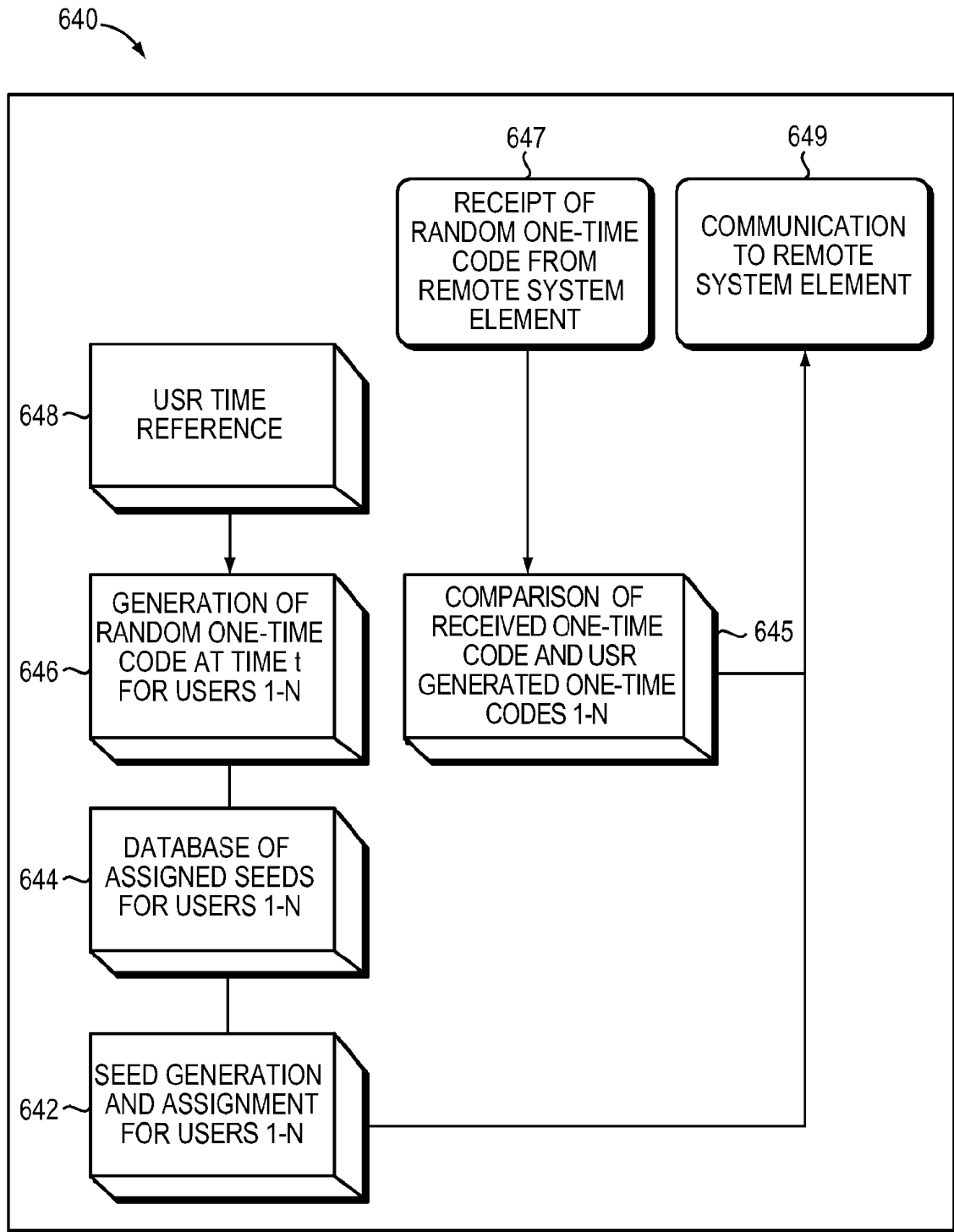


FIG. 7



8/12

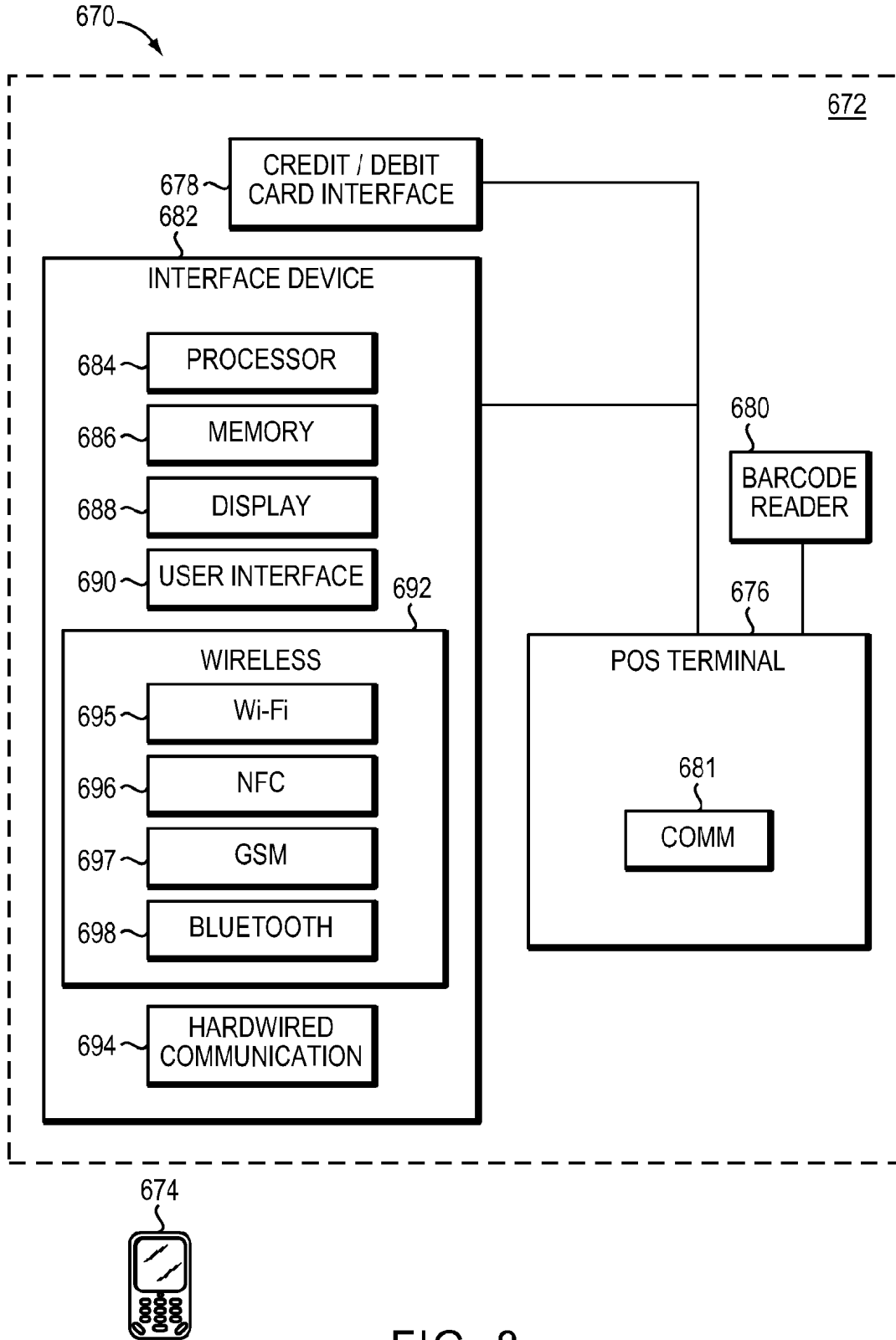


FIG. 8



9/12

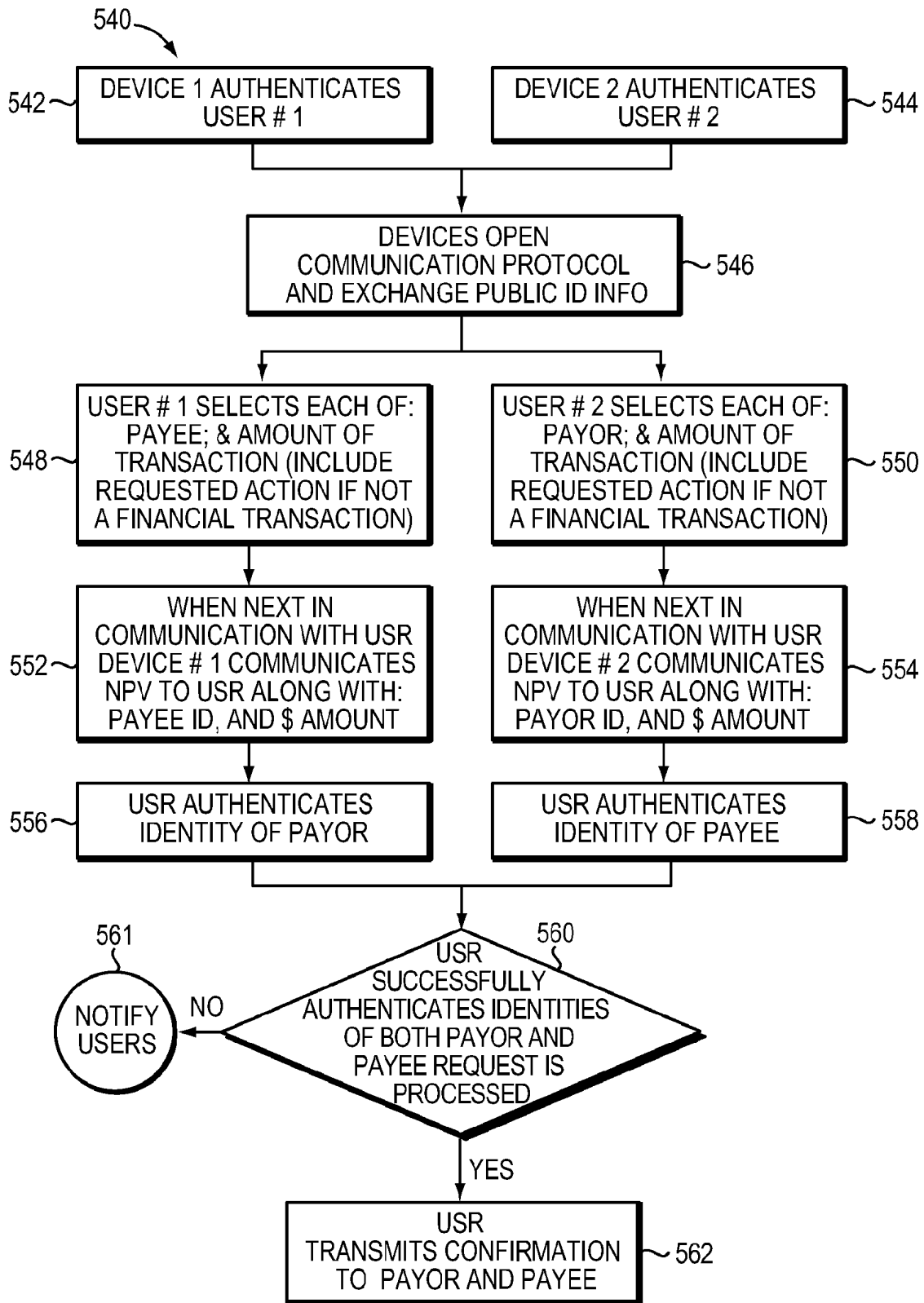


FIG. 9



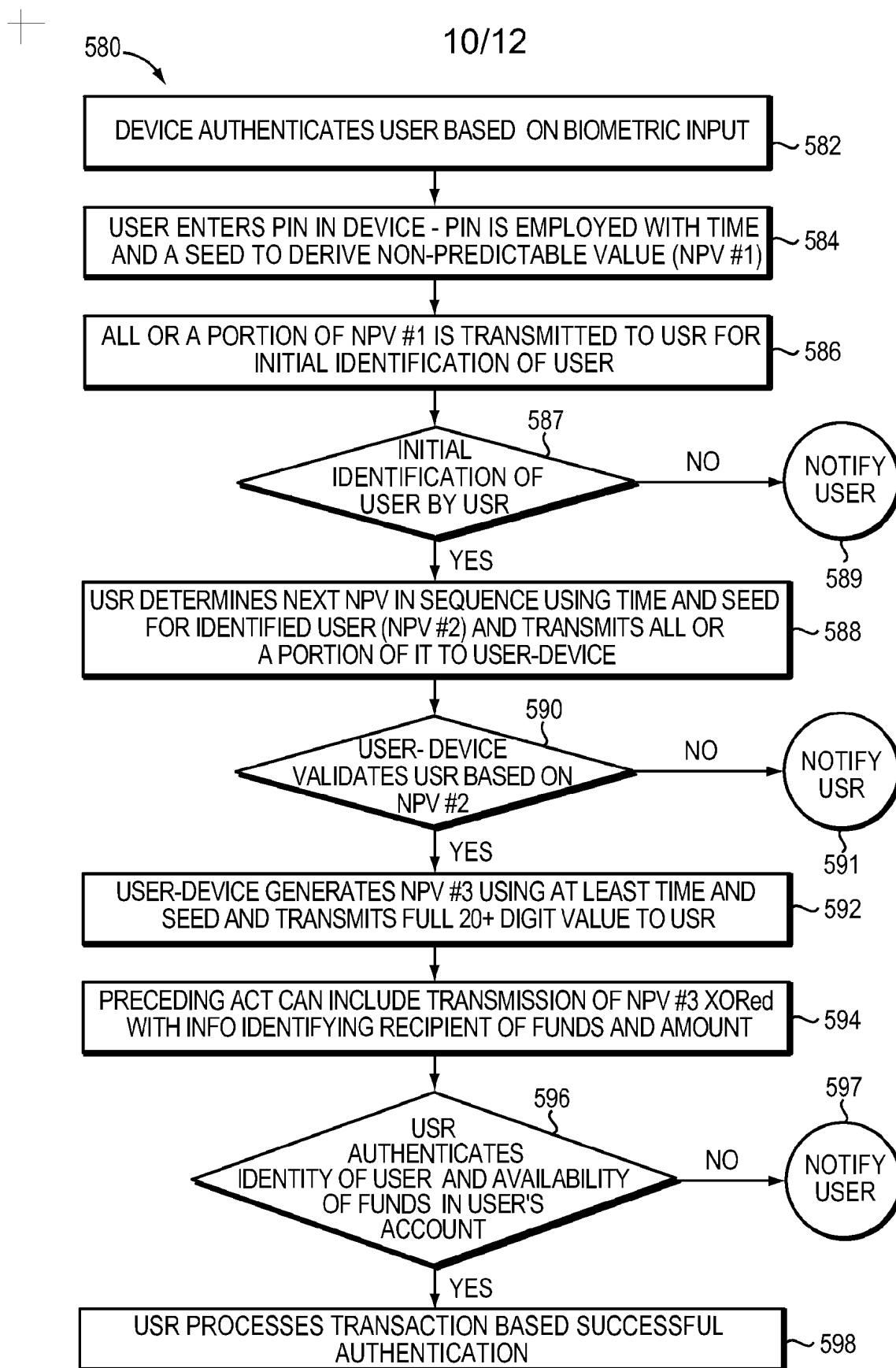


FIG. 10



11/12

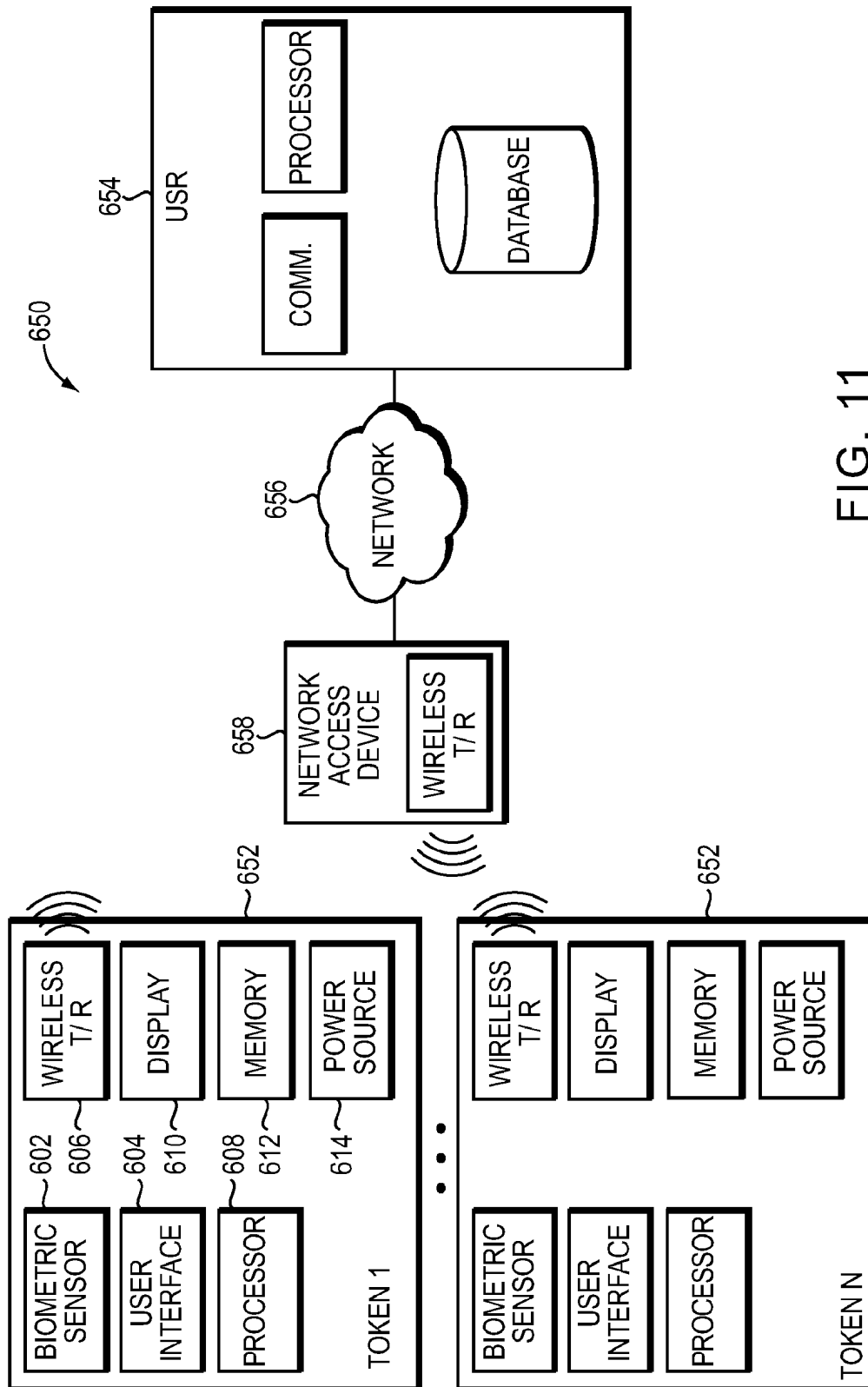


FIG. 11



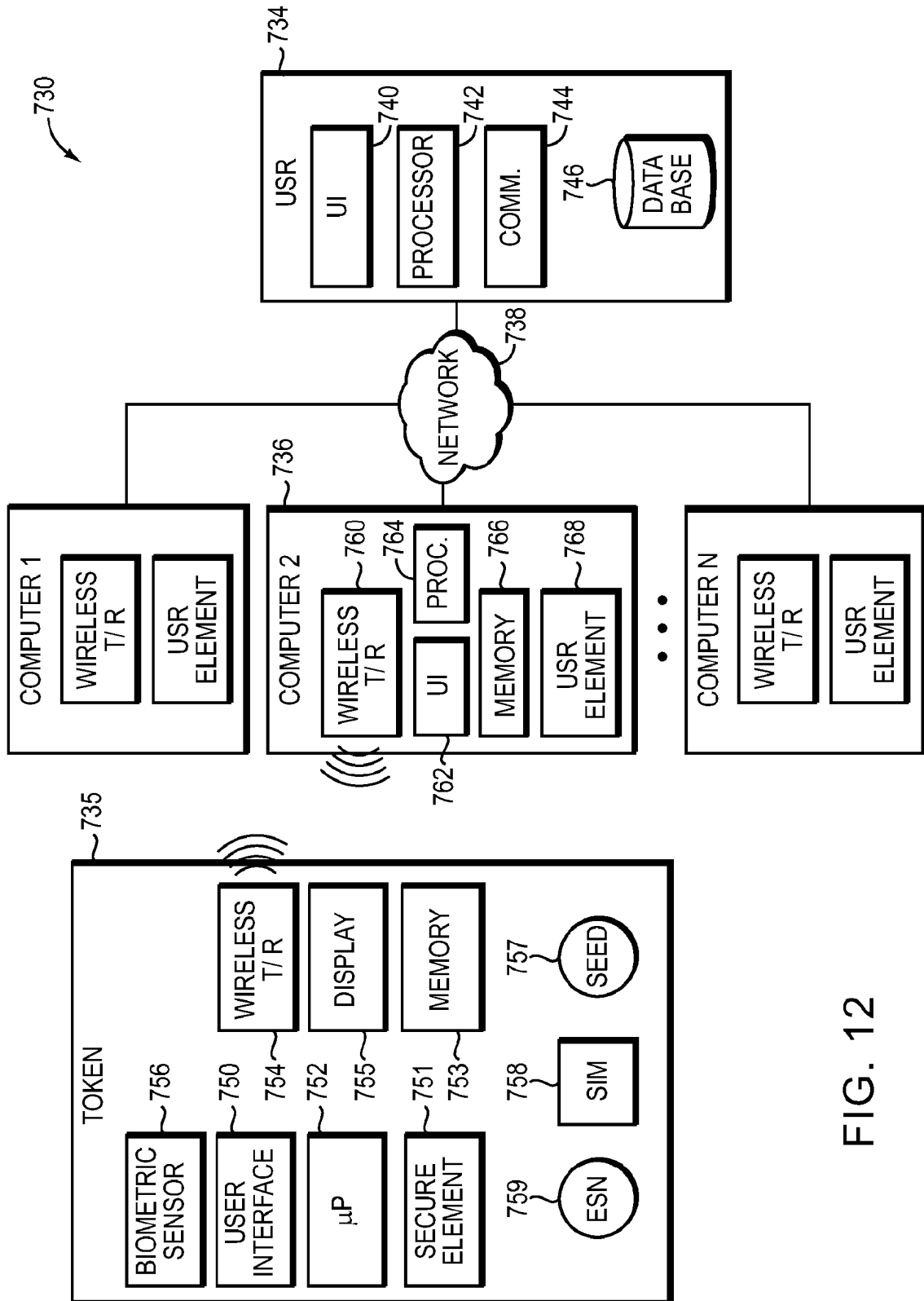


FIG. 12

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2011/051966

A. CLASSIFICATION OF SUBJECT MATTER
INV. H04L29/06 H04W12/06
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
H04W H04L

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	WO 2010/000455 A1 (VODAFONE HOLDING GMBH [DE]; MOUTARAZAK SAID [NL]; KORAICHI MAJIB [NL]) 7 January 2010 (2010-01-07) page 3, lines 6-23; claim 4 page 4, lines 28-31 page 5, lines 27-30	1-33
A	----- US 2007/186115 A1 (GAO XIANG [CN] ET AL) 9 August 2007 (2007-08-09) paragraphs [0008], [0072], [0074] -----	1-33

Further documents are listed in the continuation of Box C.

See patent family annex.

* Special categories of cited documents :

- "A" document defining the general state of the art which is not considered to be of particular relevance
- "E" earlier document but published on or after the international filing date
- "L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
- "O" document referring to an oral disclosure, use, exhibition or other means
- "P" document published prior to the international filing date but later than the priority date claimed

- "T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
- "X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
- "Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.
- "&" document member of the same patent family

Date of the actual completion of the international search

12 January 2012

Date of mailing of the international search report

20/01/2012

Name and mailing address of the ISA/

European Patent Office, P.B. 5618 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040,
Fax: (+31-70) 340-3016

Authorized officer

Veen, Gerardus

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US2011/051966

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 2010000455 A1	07-01-2010	AT 531220 T EP 2152033 A1 US 2011113476 A1 WO 2010000455 A1	15-11-2011 10-02-2010 12-05-2011 07-01-2010

US 2007186115 A1	09-08-2007	NONE	

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
21 February 2002 (21.02.2002)

PCT

(10) International Publication Number
WO 02/14985 A2

- (51) International Patent Classification⁷: G06F
- (21) International Application Number: PCT/US01/25888
- (22) International Filing Date: 17 August 2001 (17.08.2001)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:
09/641,073 17 August 2000 (17.08.2000) US
- (71) Applicant and
- (72) Inventor: KERN, Daniel, A. [US/US]; 201 East 69th Street, New York, NY 10021 (US).
- (74) Agents: YANNEY, Pierre, R. et al.; Darby & Darby P.C., 805 Third Avenue, New York, NY 10022 (US).
- (81) Designated States (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU,

CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW.

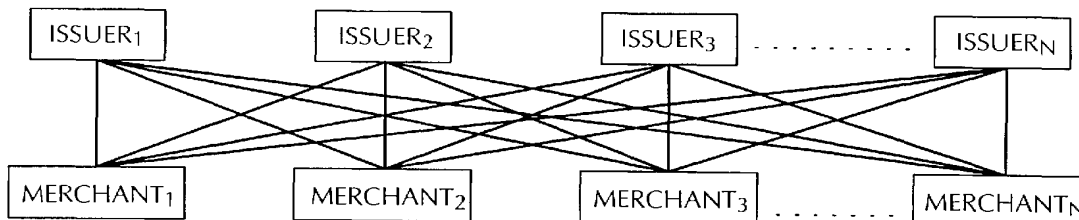
(84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— without international search report and to be republished upon receipt of that report

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.



(54) Title: AUTOMATED PAYMENT SYSTEM



(57) Abstract: An automated payment system, such as for credit cards, is provided which compiles customer financial account information from a plurality of financial institutions. The system receives account information from the financial institutions, and compiles the information in central location. The system presents financial account information to the customer. The system then receives and stores a selection of at least one of the financial accounts of the customer and provides the selected financial account information to a merchant, biller or payment processor.

WO 02/14985 A2

5

10

AUTOMATED PAYMENT SYSTEM

15

FIELD OF THE INVENTION

The present invention relates to computerized billing and payment systems. In particular, the invention relates to an automated credit card payment system that matches a customer's information, fingerprint, retina scan voice, or other biometric measurement and/or a unique personal identifier ("UPI") with financial account information consolidated from multiple financial institutions and selects, or allows customers to select, a financial account for use in paying bills, invoices and other obligations.

25

BACKGROUND OF THE INVENTION

Most companies that provide continual services can automatically bill their customers on a regular basis. To increase customer retention, as well as reliability in payments, and also to avoid the need for repeated billings of past due accounts, companies

increasingly offer customers the option of making payments through the customer's credit card. However, the need for customers to retrieve the credit card they wish to use, coupled with the customer's perception that writing their credit card account number on a bill and mailing it is not secure, hinders many customers from taking advantage of this convenient payment method.

5 Second, when a customer desires to purchase goods or services on the Internet, they usually give the merchant their credit card information as a form of payment. Since there are millions of merchants on the Internet, it is becoming increasingly difficult for the consumer and for credit card organizations to control fraud. From the moment the consumer presses "send" on the merchant's website, their credit card is exposed. Their card number can be
10 intercepted by perpetrators en route to the merchant, or it can be "hacked" from the merchant's database once it is received. In addition, the fact that there are millions of merchants and that that number is growing exponentially, makes it virtually impossible to ensure that the merchant is a legitimate company and not merely in existence to perpetrate credit card fraud.

 Third, when a customer purchases goods or services with a traditional bricks-
15 and-mortar merchant, they must have their credit card with them, and they must give it to the merchant so that the credit card can be processed. Given this conventional scenario, the consumer is vulnerable when the credit card is lost or stolen. They are also vulnerable if the merchant or any employee decides to use the credit card number in a fraudulent manner.

 Thus, there is a need for a system that provides customers the ability to
20 efficiently match their financial account information with their UPI, allowing them to purchase goods or services with their credit card or other financial account, without presenting the actual card. The aim of this system is to optimize customer security and privacy interests.

SUMMARY OF THE INVENTION

25 The present invention is for a system and related method for payment of bills, purchases, or other payments which compares a UPI or a merchant/biller's database of subscribers, customers, potential customers, prospects, or accounts receivables, sometimes referred to herein collectively as "customers", either with a consolidated database of financial account information such as credit card account information, or with a plurality of non-
30 consolidated databases of financial account information, or with a combination of the two types. Many types of financial account information may be used to make the payments,

including, but not limited to, credit cards, charge cards, debit cards, smart cards, bank cards, demand deposit accounts such as checking accounts, virtual payment accounts, virtual cash account numbers such as those provided for commercial transactions over the Internet, wire transfer networks, financial electronic data interchange (FEDI), E-check, Automated Clearing House (ACH), payment products from third party, non-bank financial institutions such as CyberCash and TransPoint (MSFDC), stored value tools such as VisaCash and Mondex, and the like.

The system matches the customer's UPI or the customer identification data contained in a merchant, biller or payment processor's database with the financial account information contained in the one or more financial account databases and selects which one or more financial accounts to present when the customer is a holder of more than one financial account.

The financial account or accounts selected are provided to the merchant or biller for inclusion on a commercial communication, such as a payment stub, renewal form, invoice, or other marketing material soliciting payment or subscription. Optionally, the merchant/biller need not know the particular financial account or number being used. For example, a commercial communication may indicate the issuer of the financial account, such as a credit card, and a particular financial account, such as a particular credit card account, for the customer to charge the purchase to, but include the account number only in encrypted form, thus offering security and privacy to the consumer. Many forms of securing information are known and may be used, including but not limited to the use of encryption techniques and record locator techniques.

For example, in a transaction where the financial account utilized is a credit card account, the customer can indicate his approval to use the credit card number provided in encrypted form and thus does not have to provide the information himself when paying by credit card. The merchant/biller collects the invoices or other offers with the customer's indication or authorization of payment from the credit card account and, optionally, submits it to a service bureau which decrypts the credit card account number and processes billing to the selected credit card account. This helps preserve the customer's privacy in his or her credit card and related information.

As shown in Fig. 2, the system of the present invention serves as an

intermediary between a large number of issuers and a large number of merchants. As shown in Fig. 2, issuers provide their account information lists to the central account management and consolidation system of the present invention, which in turn receives customer identification data from merchants, and matches and selects financial account information to provide to merchants, as described above.

In some embodiments, the system includes a memory device which stores consolidated multiple financial account information, such as a master financial account list, which includes, for example, credit card account information from multiple credit card issuers. A computer system or other processing unit matches customer identification data from the stored consolidated financial account information to a UPI or to a database of a merchant/biller's customer identification data in order to associate a financial account number with a selected member of the customer database. The computer system or processing unit selects one or more specific associated financial account numbers when more than one financial account number matches the selected member of the merchant/biller's customer database. If not previously encrypted, the associated financial account number is encrypted and provided to the merchant/biller for inclusion on the customer's commercial communication, such as a bill, payment stub, renewal form or invoice, which is then sent to the customer. After selection and authorization by the customer, the system may also decrypt the encrypted financial account number for processing payment to the merchant/biller from the selected financial account of the customer.

Alternatively, in lieu of including a master consolidated database of financial account information, the system may be comprised of a plurality of databases of financial account information either internal or remote, and a mechanism for searching the various databases to locate a customer's financial account information. The various financial account information databases may include databases of individual issuers and/or partially consolidated databases containing information from a number of financial account issuers.

A method in accordance with one embodiment of the invention includes the steps of consolidating multiple financial account information lists from multiple financial account issuers into a master financial account list, receiving a UPI or a merchant/biller's customer database, and matching information from the master financial account list to the customer's UPI or to the merchant/biller's database to associate at least one financial account number for

each customer. In accordance with desired selection rules, one or more of the matching financial account number(s) is selected, if more than one financial account number is found for a particular customer. The selected financial account number is encrypted, or may be provided already encrypted in the financial account databases. The encrypted financial account number or numbers are provided to the merchant/biller for inclusion on the merchant/biller's commercial communication to the customer, thus providing the customer with a means for authorizing payment for purchase to the associated financial account number, such as a particular credit card. Payment for the purchase is processed and made to the merchant/biller from the financial account of the authorizing member. Of course, a financial account number can be any unique encrypted identifier, even those including letters as well as numbers.

Alternatively, instead of consolidating multiple financial account information from a number of financial account issuers into a single master financial account database or list, the method may include consolidating some subset of financial account lists and searching a plurality of such lists as well as lists from individual financial account issuers in order to associate at least one financial account number for each customer in the merchant/biller's customer database, or searching a plurality of individual financial account lists made available by different issuers.

In another embodiment, the present invention is directed to a system and method for providing automated payments over a computer network, for example, over the Internet. The system includes an automated payment server which is connected to various financial institutions and which receives and compiles data from those institutions to create files of account information for various customers. When a customer desires to purchase goods from a merchant's web site, or to pay bills, the customer is routed to the payment server, and is presented with the account information as compiled by the payment server. The customer selects one or more of the financial accounts, and the payment server transmits the appropriate financial information to the merchant's payment processor to complete the transaction. In this manner, credit card numbers are not transmitted over the Internet or stored on a merchant's site, but are only transmitted between the payment server and the payment processor, preferably over a secure line.

BRIEF DESCRIPTION OF THE DRAWINGS

15 For a fuller understanding of the invention, reference is made to the following description taken in connection with the accompanying drawings, in which:

Fig. 1 is a block diagram illustrating the problems encountered in matching a large number of financial account issuers to a large number of merchants/billers in an automated payment system;

20 Fig. 2 is a block diagram illustrating the use of the present invention in efficiently matching a large number of financial account issuers to a large number of merchants/billers in an automated payment system;

Fig. 3 is a block diagram of a preferred embodiment of an apparatus for carrying out the automated credit card payment method and system of the present invention;

25 Fig. 4 is a flow chart illustrating the use of the apparatus of Fig. 3;

Fig. 5 is a block diagram of an alternative embodiment of the present invention;

Fig. 6 is a block diagram of an automated payment system used for billers in accordance with one preferred embodiment of the invention;

Fig. 7 is a flow chart illustrating the use of the system of Fig. 6;

30 Fig. 8 is a block diagram of an alternative embodiment of the present invention;

Fig. 9 is a flow chart illustrating the use of the system of Fig. 8;

Figs. 10 and 11 are representations of an interface presented to a customer upon accessing a payment server according to one aspect of the invention; and

Fig. 12 is a block diagram of an embodiment of an apparatus for carrying out the automated credit card payment method and system of the present invention using a bricks-and-mortar terminal and a biometric identifier and/or PIN.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Preferred embodiments of the invention are now described with reference to the drawings. Although many of the drawings and descriptions illustrate the use of the invention with credit card accounts for the sake of simplicity, the invention is in no way meant to be limited to credit card accounts.

Referring to Fig. 3, an automatic payment system 50 according to one embodiment of the present invention is shown. The system 50 may utilize any combination of many types of financial accounts and is described with reference to credit card accounts for simplicity. The system 50 may be operated by a company, such as a service bureau, and includes a database consolidation and sorting subsystem 55, a master credit card database 57, an identifier matching and selecting subsystem 59, and an optional credit card account number encryption subsystem 53.

The automatic payment system 50 is used in conjunction with n number of credit card issuers 60_0 to 60_n . Each of the n credit card issuers 60 maintains on a computer system its own credit card information list 66_0 to 66_n in accordance with one of a number of conventional format types known to those of skill in the art. These credit card information lists 66 typically contain account holder identification data, such as the name and address of each account holder, as well as the associated credit card number, name of financial institution, account information and demographic information pertaining to each card holder. One skilled in the art will recognize that although the preferred embodiments are described with reference to the use of credit cards, other financial account information or devices, including but not limited to smart cards, bank cards, checking accounts, and virtual payment accounts used for Internet and other on-line commercial transactions, may be used instead of or in any combination with credit card accounts.

The automated payment system 50 receives credit card information lists 66 over

a transmission medium 68 from the n credit card issuers 60. This transfer of information over medium 68 may be achieved by many communications methods, including but not limited to modem connections, high speed data lines, the Internet, or the physical transfer of storage media, such as tapes or disks. This transfer is authorized by contractual relationships and may include financial incentives. In order to increase the likelihood of locating customer credit card information, it is preferable to include the credit card account information from as many credit card issuers as possible. The database consolidation and sorting subsystem 55, which may be in the form of a programmed computer system, sorts and consolidates the credit card information 66_o to 66_n provided by the credit card issuers 60_o to 60_n, and the sorted and consolidated data is then stored in the master credit card information database 57. This database may reside on a mass storage unit of the computer system. Of course, the processing elements and information storage elements may reside on multiple computing devices to provide for contingencies such as fault tolerance and load balancing.

The automated payment system 50 is used to provide credit card account information to one or more of m number of merchants/billers 70_o to 70_m. Each of the m merchants/billers may maintain on a computer its own list 76 of customer identification data. These lists 76_o to 76_m include customer identification data such as names and addresses of customers or additional information, such as social security numbers and demographic information. The automatic payment system 50 receives the customer identification data from a given merchant/biller 70_x, and the matching and selecting subsystem 59 compares the customer identification data supplied by merchants/billers 70_x with the records in the master credit card information database 57 to locate matching credit card holder identification data. The matching and selecting subsystem 59 may be in the form of a preprogrammed computer system which is either the same as the one used for the database consolidation and sorting subsystem 55, or separate therefrom. The process of matching customers from a merchant/biller database to credit card account holders in the matching and selecting subsystem 59 may be performed using conventional matching algorithms as known to those of skill in the art.

If more than one credit card holder identifier matches a given customer (i.e., the customer has more than one credit card), one or more of the matching credit card identifiers is selected or featured by the matching and selecting subsystem 59. This selection

proceeds in accordance with certain selection and presentation rules. As an illustrative example, a simple selection rule is used wherein the selected credit card is the one issued by the issuer having the most credit cards in the database, i.e., the most “popular” or predominant credit card. Alternatively, in one embodiment, the selection is made on a pro rata basis or 5 other algorithm based on the total number of credit card accounts for each issuer in relation to the number of credit card accounts for the other issuers and the total number of credit card accounts in the master credit card database 57. Thus, for example, a credit card issuer which accounts, for example, for 25% of the total number of credit card accounts in the consolidated database, will have its associated credit card account selected 25% of the time for customers 10 who have multiple credit card number accounts including that issuer. Another method of selecting one associated credit card account number from more than one matching associated credit card account is to compare the selected associated credit card account numbers with credit card usage information to determine the customer's primary credit card, based on amount of use, and selecting the customer's most often used credit card. Yet another method 15 of selecting an account may take into consideration the fees associated with financial transactions and select the financial institution that charges the lowest fees. Alternatively, the selection process may take into account historical data and select the financial institution that yields the best results or success for a particular merchant/biller. Finally, the selection may be made as a result of fees paid by the credit card issuer to receive priority in the selection 20 process.

In alternative embodiments, more than one credit card, or all of the credit cards, may be selected for inclusion, and the customer is given the option of selecting which one of the cards is to be used for making payment. In this embodiment, all matching credit card account numbers may be selected and presented to the customer. The selected credit card 25 accounts may be presented to the customer in a list with a check box, such as in the following form:

Choose the card(s) with which you wish to pay:

_____ CITIBANK VISA

_____ DISCOVER

30 _____ AMERICAN EXPRESS

In a more preferred embodiment of the present invention, the selected credit card accounts can also be ordered and presented to the user, based on similar criteria as that used by the system to determine the selection of credit cards, *e.g.*, the most popular card in the database, the customer's most often used credit card, the card that charges the lowest fees, or the card whose issuer has paid the highest fee, can be presented above or ahead of other credit cards.

The selected credit card account number or numbers which are to be included on a commercial communication are encrypted by a credit card account number encryption subsystem 53. The particular method of encryption may include a finder number, record locator, some form of high level encryption, or any other encryption technique. While encryption is an element of the preferred embodiment, the method of encryption may be any method which achieves adequate security and the specific method of encryption does not constitute a material element of the system and method set forth herein. Moreover, credit card information may be encrypted and provided in encrypted form from the credit card issuers before being stored in the master credit card information database.

Fig. 4 illustrates the use of encrypted account information of the present invention, and specifically, encrypted credit card information for the sake of simplicity. In one embodiment, for each customer in a merchant/biller's customer identification data database 76, the encrypted credit card account number associated with the customer is provided by merchant/biller 70_x to the customer (step 80) as part of the communication to the customer from merchant/biller 70_x. Alternatively, in a bricks-and-mortar embodiment of the present invention where the bricks-and-mortar merchant does not have a "customer information database," the customer communicates directly to the central database 57 via a payment process interface, *e.g.*, a terminal or computer. At step 90, the customer decides whether to authorize payment by credit card. This authorization step may also include selecting which credit card(s) to use if the customer is presented with more than one. If the customer authorizes such payment and returns the commercial communication to the merchant/biller or other payment processing entity, the encrypted credit card account number is decrypted at step 100. The encrypted number may be sent by the system 50 to the credit card issuer, a payment processor or merchant for decryption and/or payment processing. After decryption the credit card account number is used to process payment to merchant/biller (step 110) and payment is made to the particular merchant/biller, along with any required payments for use of the system

in handling the transaction. If the customer 90 does not authorize payment, steps 100 and 110 are simply not performed.

It should be understood that elements of the system and method of the present invention described herein, such as in Figures 3 and 4, may be modified in keeping with the intended scope of the invention. For example, the consolidated credit card account database has been described as containing account information from multiple credit card account issuers. However, the merchant/biller's customer identification data may alternatively be matched serially against multiple databases, including individual credit card issuers' credit card account databases and/or one or more consolidated database. Each individual or consolidated database represents some number of credit card issuers which is a subset of all the issuers.

Fig. 5 shows an alternative embodiment of an automated payment system 50' according to the present invention. The system 50' of this alternative embodiment includes a serial matching subsystem 59' and a selection/presentation subsystem 59''. The serial matching subsystem compares customer identification data, received over transmission medium 1569 from a merchant or one or more customer databases 76 of a given merchant/biller 70, to a number of credit card databases 66 of a number of issuers 60. The serial matching subsystem may also compare the customer identification data with a consolidated database 58 containing information consolidated from a limited number of issuers 60, in this case, issuers 3 and 4. The serial matching subsystem locates matches of the merchant/biller's customer identification data with account holder identification data contained in the individual and partially consolidated databases 66 and 58, as discussed above. Once a set of matching credit card account numbers is located, the selection subsystem 59'' selects one or more of the account numbers, in accordance with the selection rules discussed above.

Referring now to Fig. 6, therein is shown a block diagram of an embodiment of the automated credit card payment system of the present invention as applied to merchant/billers. In this arrangement, multiple merchant/billers 150 use a fulfillment house 152 and a service bureau 154 employing the system of the present invention to deal with multiple credit card account databases 156, one or more of which may be partially consolidated databases as explained above. More than one fulfillment house 152 may be utilized to serve the various merchant/billers and/or groups of merchant/billers, or one fulfillment house 152 may be used for each biller 150. Merchant/billers 150 provide the fulfillment house 152 with

each of their customer files 158 and outside lists 160 (e.g., lists of prospective customers). The service bureau 154 uses the system of the present invention to match the names on the merchant/billers' customer files 158 with associated financial account information. This information, including credit card information, is consolidated by the service bureau 154 from multiple credit card issuers 156 and is stored in a master credit card file. Alternatively, this credit card information can be accessed serially from databases of the multiple credit card issuers.

After matching the merchant/billers' customer files 158 and outside lists 160 with associated financial account information, the service bureau encrypts the matching credit card account numbers (block 162) and provides them to the fulfillment house 152. The use of the located credit card information is shown in the flow chart of Fig. 7, where fulfillment house 152 uses the encrypted credit card account information in marketing, billing and/or renewal efforts (step 164), such as by placing encrypted credit card account numbers on commercial communications. At step 165, customers authorize the use of their credit card, and optionally select which credit card to use if more than one is presented to the customer.

When customers place orders using the encrypted credit card account information on the commercial communication, the orders are collected and the encrypted number entered and consolidated into a consolidated order file (step 166). The encrypted account numbers in the consolidated order file are then decrypted (step 170) and payments are processed (step 172).

Referring now to Figs. 8 and 9, there is shown another embodiment of the present invention. In this embodiment, the system 200 is designed for use over a computer network, for example, over the Internet, a LAN, WAN, or the like. The system 200 includes an automated payment server 202 that includes a processing unit 204 and a customer database 206 maintained by the processing unit, and is similar in many respects to the automated payment system 50 described above. The database combines account information from various financial institutions, as well as bill information from various billers.

The automated payment server 202 connects to a plurality of customers at respective terminals 208, and interacts with those customers via a suitable customer interface 210 (only one terminal is shown schematically in FIG. 8). The customer interface can be a basic application used to select payment options, a method of viewing bills from various

billers, and/or a full-service interface that combines those functions and allows the customer to re-configure the account. It will be apparent to those skilled in the art that various forms of interface may be employed.

The automated payment server 202 further connects to one or more merchant sites 212 over one or more communication lines 214. Preferably, at least one of the lines 214 is a secure line for transmission of payment information, as is described in greater detail below.

The automated payment server 202 is connected to various financial institutions 220 and to various billers 222. The automated payment system 202 receives account information, including updated account information, over a transmission medium from the financial institutions, and receives billing information from the various billers, as described above in connection with the automated payment server 50. For example, various utilities may transmit bills electronically to their customers via the payment server 202. An automated account information merge/purge subsystem 224 and an automated bill information merge/purge subsystem 226, which may be in the form of programmed computer systems, sort and consolidate the account and bill information provided by the financial institutions and billers, and the sorted and consolidated data is then stored in the customer database 206 for subsequent access, as is described in greater detail below.

The customer terminals 208 can take many different forms, and can access the automated payment server 202 in many different ways. For example, the customer may transmit purchase requests via a brick-and-mortar terminal, E-mail, or over the Internet by clicking on a banner on a web site, through interactive television, WebTV®, over the telephone, by direct mail, or in any other suitable manner. In one embodiment, the merchant site 212 may post a banner indicating that payment for a transaction may be conducted through the automated payment server 202. The customer can then click on the banner and be directed to the automated payment server, as is described in greater detail below.

The customer interface 210 is preferably a suitable interface that allows the automated payment server 202 to simultaneously communicate with multiple customers over the Internet or other computer network.

Referring now to Fig. 9, the operation of the automated payment server 202 is described in more detail. Operation begins at step 300, with a customer beginning the

transaction by communicating with a merchant 212 and either placing an order or requesting to pay a bill for goods or services. In one embodiment, the merchant site presents the customer with a banner having an embedded URL of the automated payment server 202, or alternatively the merchant site can automatically direct the customer to the automated payment server when the customer places an order. At step 302, the customer is linked to the automated payment server 202, and at step 303 the server determines whether the customer is registered with the server. If the customer is not registered, operation proceeds to step 304, and the customer registers with the payment server. Registration can be conducted over the computer network, over the telephone, through the mail, or in any other suitable manner, and involves receiving identifying information from the customer to verify the identity of the customer for all subsequent transactions. For example, the customer may provide their name, address, etc., along with their mother's maiden name, a social security number, or the like. The customer may also provide biometric information, *e.g.*, fingerprint sample, handwriting sample, retina scan, or voice recording/pattern. Once the customer's identity has been verified, a password is selected for the customer (either chosen by the customer or randomly assigned by the payment server), as is well known in the art.

If the customer is already registered with the payment server 202, the customer inputs his or her user name and password at step 303, and after authentication or verification, the customer is allowed to continue with the payment transaction.

The merchant 212 transmits order and/or payment data to the payment server 202, either automatically or after being prompted by the payment server, at step 305. The data preferably identifies the customer, for example by including order ID data and/or a customer UPI, which is also transmitted to the payment server when the customer accesses the payment server. Alternatively, the merchant site may transmit the customer's name or any other identifying data to allow the payment server to associate the customer with the particular order or payment request.

The customer's UPI or other identifying information is associated with the customer's financial account(s). The UPI can be in the form of a name, password, PIN, ID number, or other unique identifier. Alternatively, the UPI can take the form of a fingerprint, retina scan, voice pattern, handwriting sample, or other unique "biometric" identifier. These biometric identifiers, in some cases, can be used in conjunction with a password or PIN. The

recording, capturing, and storing of unique biometric identifiers such as retina scans, iris scans, voice patterns, digital handwriting samples or digitally scanned fingerprints are described in U.S. Patent Nos. 6,047,281; 6,038,334 and 5,991,408, the disclosures of which are incorporated herein by reference. In one possible embodiment of the invention, the customer's UPI is recorded and/or authenticated using prior art devices, such as digital scanners, cameras or recorders, attached to the consumer's computer or located at a bricks-and-mortar or other merchant terminal as exemplified in Fig. 12.

Once the payment server has associated the customer with the order or payment request, operation proceeds to step 306, and the payment server accesses the customer database to retrieve the customer's account information, which as described above is in the form of various credit cards, debit cards, smart cards, bank cards, demand deposit accounts such as checking accounts, virtual payment accounts, wire transfer networks, financial electronic data interchange (FEDI), Echeck, Automated Clearing House (ACH), payment products from third party, non-bank financial institutions such as CyberCash and TransPoint (MSFDC), stored value tools such as VisaCash and Mondex, and the like. Then, at step 308, the payment server presents the customer account information to the customer (Fig. 10). The account information identifies the various financial to the customer, without transmitting entire account numbers to the customer. For example, some identifying information is transmitted, such as the name of the credit card, the last several digits of a credit card, or the like (e.g., "AmEx 206543"). The account information may include, in addition to identifying the various credit cards and the like, available balance information, date of the last update to that account, date of last payment, credit limit, transaction detail, and the like.

At step 310, the customer selects one or more payment options, and that selection (or selections) is transmitted to the payment server via the interface 210. Thus, the actual account numbers are not transmitted between the payment server and the customer.

The customer may choose to split a payment between two or more financial accounts, for example, two or more credit cards. In addition, the payment server can present the accounts to the customer in some specific order, as defined by the customer, the financial institutions, particular merchants, account usage, available balances, interest rates, and the like.

In one embodiment, the payment server 202 presents the customer only with

appropriate payment options. For example, if the purchase amount is \$100, and the customer's checking account has a balance less than \$100, the payment server preferably does not provide that as an option to the customer. Alternatively, the checking account may be presented to the customer, but in a different color or font to indicate to the customer that such account is not suitable for the particular transaction, but can be used in connection with another payment option to complete the transaction.

At step 312, the payment server 202 transmits a request for authorization to the payment processor of the merchant site 212, which includes the payment option selected by the customer. At step 314, the customer interface determines whether the payment option is acceptable. For example, the customer may have selected a credit card that is not accepted by the particular merchant. If so, operation proceeds to step 316, and the customer is informed that the authorization failed. Operation then flows back to step 308, to allow the customer to select another payment option.

If the payment option is acceptable at step 314, operation proceeds to step 318, and the customer is notified that the transaction has been approved. Then, at step 320, the payment server 202 transmits the approved order or Approval to the merchant site or to the merchant's payment processor 212, preferably over a secure line, and the merchant fills the order by interacting with the customer 208. For example, the merchant site may request shipping information if they do not already have it or other required information to complete the transaction. Then, at step 322, the payment processor accesses the appropriate financial institution and transmits the payment information, so that the customer's account is debited and the merchant's account is credited.

It will be apparent to those skilled in the art that the above steps may also be carried out over a telephone network that allows for interactivity, such as those systems offering voice recognition and/or dual tone multi-frequency (DTMF) tones. As is well known in the art, the customer may enter a user ID and password by pressing the appropriate keys on the telephone, with the payment server including the appropriate, well-known hardware to interpret the DTMF tones to determine the corresponding numbers entered by the customer. Thus, a customer may dial a telephone number, listen to a list of available goods, services and/or bills, and select one or more of the goods, services and/or bills by pressing appropriate keys on the telephone. The payment server, through a well-known interactive system such as

interactive voice response (IVR) or the like, then prompts the customer to enter identification data, such as a user name and PIN number, or the like. Once the identity of the customer is verified, the payment server may then present the customer with a list of credit cards that may be used to complete a transaction. For example, the IVR software may read "Press 1 to select your Visa account, press 2 to select American Express," or the like. The customer may simply press the corresponding key on the telephone to signal the payment server of the customer's choice. The remainder of the process is the same as the computer network version described above. Thus, in this manner the payment server 202 is available to customers over a telephone network.

10 Alternatively, the present invention may be implemented through the mail, by the customer returning an order form sent through regular mail and/or electronic mail. In this manner, the payment server sends a preprinted order form to potential customers, listing various goods, services and/or bills available, and also listing that particular customer's financial accounts as compiled by the customer database 206. The customer selects one or
15 more of the goods, services and/or bills, selects a financial account for payment from the customer-specific list printed on the form, and returns the order form to the payment server 202. An operator at the payment server then enters the data, or in the case of electronic transfer such as email, the data is uploaded. The payment server forwards the data to the appropriate merchant. If the payment option selected by the customer is not appropriate (e.g.,
20 the merchant does not accept that type of payment or the available balance is too low), the customer is notified, either through the mail (electronic or regular) or via telephone, and may select another payment option. Once a suitable payment option is selected, the remainder of the transaction is completed along the lines of the computer network version described above.

In an alternative embodiment, the customer who receives the order form or bill
25 may call a telephone number provided on the form and complete the transaction over the telephone, in the same manner as described above.

In another embodiment, the customer at terminal 208 may access the payment server 202 directly without initially accessing a merchant's site. The customer then may be presented with outstanding bills, as compiled by the automated bill information merge/purge
30 subsystem 226 (Fig. 11). The customer may select one or more of the bills to be paid, and is then presented with the account information, similar to the process described above with

respect to Fig. 9.

It will be apparent that the system and method of the present invention allow payment transactions to be performed over a computer network without requiring any credit card numbers or the like to be transmitted directly between the customer 208 and merchant 5212, or between the customer 208 and the payment server 202. Thus, no account information passes over a public network such as the Internet. The account information is transmitted over secure lines between the financial institutions and the payment server 202, and between the payment server and the merchant's payment processor or the merchant's site. In addition, multiple merchants do not need to maintain a database of account numbers, as such information 10 is maintained at the payment server 202. Maintaining the database at one location rather than at each individual merchant further reduces the likelihood of fraud.

Referring to Fig. 12, an automatic payment system 50 is shown according to an embodiment that implements use of biometric identifiers and/or PINs. A biometric identifier and/or PIN is collected at a bricks-and-mortar terminal. A bricks-and-mortar terminal may 15 include a computer, digital camera, scanner, recorder or other device capable of capturing such information. The automatic payment system 50 receives the biometric identifier and/or PIN from the bricks-and-mortar terminals 84_x, and the matching and selecting subsystem 59 compares the biometric identifier and/or PIN 88_x with the records in the master credit card information database 57 to locate matching credit card holder identification data. The matching 20 and selecting subsystem 59 may be in the form of a preprogrammed computer system which is either the same as the one used for the database consolidation and sorting subsystem 55, or separate therefrom. The process of matching customers from a merchant/biller database to credit card account holders in the matching and selecting subsystem 59 may be performed using conventional matching algorithms as known to those of skill in the art. If a match is 25 found in the master credit card database 57, then the PIN is validated.

As can be understood from the above description of the present invention, the present invention provides a number of benefits to customers (such as credit card users), financial institutions, merchants and billers. Benefits for the financial institutions include reduced fraud, more credit card usage, higher retention rates, and increased fee income. 30 Benefits for the customer include convenience, privacy, and efficiency. Benefits to the merchant/billers are reduced fraud and theft, higher retention rates, less bad debt, savings on

mailing expense, and better customer relationships.

The system and method of the present invention may also be used in conjunction with a targeted marketing or coupon plan in which purchasing behavior can be identified and recorded by the payment server. In one possible embodiment, consumers with financial accounts (including credit card accounts) on the payment server can acquiesce in having their purchasing behavior tracked and provided to a wide variety of businesses and industries. These business and industries can then preferentially target various consumers for discounts, coupons, or other marketing deals based on their past purchases.

Another benefit provided by the present invention is the security and privacy for consumers. Therefore, in accordance with the preferred embodiment of the invention herein, a centralized organization or company is the only party, aside from the financial institutions with relationships with the consumers, as well as the consumers themselves, that has access to the specific financial account information. It should be understood that the functions performed by the central organization may actually be divided between separate entities. For example, one entity may perform processing, while another entity performs encryption/decryption. As described above, only encrypted account information is provided to the merchants/billers; however, it is within the scope of the present invention to provide a system in which accounts are provided to merchants/billers directly, and the merchant/biller or other company encrypts such account information for use in its billing materials. In such a case, once the merchant/biller receives the customer's approval for charging a particular account, it can proceed to decrypt and process the payment from the financial institution directly.

Many other user functions known in the art can be implemented such as the ability to allow a user to modify his user registration information.

While several forms of the invention have been described, it will be apparent to those skilled in the art that various modifications and improvements may be made without departing from the spirit and scope of the invention.

WHAT IS CLAIMED IS:

1. A method for facilitating payment from a customer's financial account to a merchant/biller or a payment processor associated with a merchant/biller, comprising the steps of:

compiling in a memory financial account information for at least one customer from a plurality of financial institutions;

receiving and storing transaction information relating to a particular customer;

retrieving from the memory the financial account information for the customer;

presenting the financial account information to the customer;

receiving and storing a selection by the customer of at least one of the financial accounts; and

providing the selected financial account(s) information either to the merchant/biller or to a payment processor associated with the merchant/biller.

1 2. The method of claim 1, wherein said financial account corresponds to at
2 least one of a credit card, charge card, debit card, smart card, bank card, demand deposit account,
3 checking account, virtual payment account, virtual cash account, wire transfer networks, financial
4 electronic data interchange (FEDI), Echeck, Automated Clearing House (ACH), and stored value
5 tools.

1 3. The method of claim 1, further comprising the step of consolidating at
2 least two of said plurality of financial account information databases into a single consolidated
3 financial account information database and wherein said retrieving step includes the step of
4 searching said consolidated database.

1 4. The method of claim 1, further comprising the steps of selecting a subset
2 of one or more financial accounts from among a plurality of customer financial accounts, and
3 presenting the subset to the customer.

1 5. The method of claim 4, wherein the subset of accounts includes financial
2 accounts acceptable to the merchant/biller.

1 6. The method of claim 1, further comprising the step of dividing payment
2 for a single transaction among more than one financial account if more than one financial account
3 is selected.

1 7. The method of claim 1, further comprising the step of selecting the order
2 in which one or more financial accounts are presented to the customer before presenting the
3 financial account information to the customer.

1 8. The method of claim 1, further comprising the steps of encrypting said
2 selected customer financial account information prior to providing it to said merchant/biller, or
3 payment processor, and encrypting or truncating the financial account information before it is
4 presented to the customer.

1 9. The method of claim 1, further comprising the step of updating said
2 financial account information from at least one of said plurality of financial institutions.

1 10. The method of claim 1, further comprising the steps of determining
2 whether a customer is a registered customer; and
3 registering a customer if the customer is not yet registered.

1 11. The method of claim 10, wherein the step of registering a customer further
2 includes capturing a PIN and a biometric measurement of the customer.

1 12. The method of claim 11, wherein the biometric measurement includes
2 voice patterns, fingerprints, retina scans, or handwriting samples.

1 13. The method of claim 11, further comprising the step of comparing the PIN,
2 biometric measurement, or both, against a respective stored database of PINs or biometric
3 measurements.

1 14. The method of claim 1, further comprising the step of comparing a
2 transaction value from the transaction information to an available balance value from the
3 financial account information.

1 15. The method of claim 14, further comprising the step of presenting to
2 customers only those financial accounts with an individual or combined available fund balance
3 equal to or greater than the transaction value.

1 16. A method for facilitating payment from a customer's financial account for
2 a bill selected from a plurality of bills presented to the customer, the method comprising the
3 following steps:

4 compiling in a memory financial account information for at least one
5 customer from a plurality of financial institutions;

6 presenting the customer with bill information for each of a plurality of
7 bills;

8 receiving selection information from the customer specifying a particular
9 selected bill which is to be paid;

10 retrieving from the memory the financial account information for the
11 customer;

12 presenting the financial account information to the customer; and

13 receiving selection information from the customer specifying a particular
14 account to be used to pay the selected bill.

1 17. The method of claim 16, wherein said financial account corresponds to
2 at least one of a credit card, charge card, debit card, smart card, bank card, demand deposit
3 account, checking account, virtual payment account, virtual cash account, wire transfer networks,
4 financial electronic data interchange (FEDI), Echeck, Automated Clearing House (ACH), and
5 stored value tools.

1 18. The method of claim 16, further comprising the step of consolidating at
2 least two of said plurality of financial account information databases into a single consolidated
3 financial account information database and wherein said retrieving step includes the step of
4 searching said consolidated database.

1 19. The method of claim 16, further comprising the steps of selecting a subset
2 of one or more financial accounts from among a plurality of customer financial accounts, and
3 presenting the subset to the customer.

1 20. The method of claim 19, wherein the subset of accounts includes financial
2 accounts acceptable to the merchant/biller.

1 21. The method of claim 16, further comprising the step of dividing payment
2 for a single transaction among more than one financial account if more than one financial account
3 is selected.

1 22. The method of claim 16, further comprising the step of selecting the order
2 in which one or more financial accounts are presented to the customer before presenting the
3 financial account information to the customer.

1 23. The method of claim 16, further comprising the steps of encrypting said
2 selected customer financial account information prior to providing it to said merchant/biller, or
3 payment processor, and encrypting or truncating the financial account information before it is
4 presented to the customer.

1 24. The method of claim 16, further comprising the step of updating said
2 financial account information from at least one of said plurality of financial institutions.

1 25. The method of claim 16, further comprising the steps of determining
2 whether a customer is a registered customer; and
3 registering a customer if the customer is not yet registered.

1 26. The method of claim 25, wherein the step of registering a customer further
2 includes capturing a PIN, an IP address or a biometric measurement of the customer.

1 27. The method of claim 26, wherein the biometric measurement includes
2 voice patterns, fingerprints, retina scans, or handwriting samples.

1 28. The method of claim 26, further comprising the step of comparing at least
2 one of the PIN, IP address, biometric measurement, against a respective stored database of PINs,
3 IP addresses or biometric measurements.

1 29. The method of claim 16, further comprising the step of comparing a
2 transaction value from the transaction information to an available balance value from the
3 financial account information.

1 30. The method of claim 29, further comprising the step of presenting to
2 customers only those financial accounts with an individual or combined available fund balance
3 equal to or greater than the transaction value.

1 31. A method for facilitating payment from a customer's financial account to
2 a merchant/biller or a payment processor associated with a merchant biller over a computer
3 network, comprising the steps of:

4 compiling in a memory at a payment server financial account information
5 for at least one customer, said information being received from a plurality of financial
6 institutions;

7 receiving over the computer network transaction information at the
8 payment server relating to a particular customer and storing the transaction information;

9 retrieving from the memory the financial account information for the
10 customer;

11 transmitting the financial account information over the computer network
12 to the customer;

13 receiving over the computer network a selection by the customer of one
14 or more of the financial accounts and storing the selection; and

15 transmitting the selected financial account information over the computer
16 network to said merchant/biller or a payment processor associated with the merchant/biller.

1 32. The method of claim 31, wherein said financial account corresponds to
2 at least one of a credit card, charge card, debit card, smart card, bank card, demand deposit
3 account, checking account, virtual payment account, virtual cash account, wire transfer networks,
4 financial electronic data interchange (FEDI), Echeck, Automated Clearing House (ACH), and
5 stored value tools.

1 33. The method of claim 31, further comprising the step of consolidating at
2 least two of said plurality of financial account information databases into a single consolidated
3 financial account information database and wherein said retrieving step includes the step of
4 searching said consolidated database.

1 34. The method of claim 31, further comprising the steps of selecting a subset
2 of one or more financial accounts from among a plurality of customer financial accounts, and
3 presenting the subset to the customer.

1 35. The method of claim 34, wherein the subset of accounts includes financial
2 accounts acceptable to the merchant/biller.

1 36. The method of claim 31, further comprising the step of dividing payment
2 for a single transaction among more than one financial account if more than one financial account
3 is selected.

1 37. The method of claim 31, further comprising the step of selecting the order
2 in which one or more financial accounts are presented to the customer before presenting the
3 financial account information to the customer.

1 38. The method of claim 31, further comprising the steps of encrypting said
2 selected customer financial account information prior to providing it to said merchant/biller, or
3 payment processor, and encrypting or truncating the financial account information before it is
4 presented to the customer.

1 39. The method of claim 31, further comprising the step of updating said
2 financial account information from at least one of said plurality of financial institutions.

1 40. The method of claim 31, further comprising the steps of determining
2 whether a customer is a registered customer; and
3 registering a customer if the customer is not yet registered.

1 41. The method of claim 40, wherein the step of registering a customer further
2 includes capturing a PIN, IP address or a biometric measurement of the customer.

1 42. The method of claim 41, wherein the biometric measurement includes
2 voice patterns, fingerprints, retina scans, or handwriting samples.

1 43. The method of claim 41, further comprising the step of comparing at least
2 one of the PIN, IP address, and biometric measurement, against a respective stored database of
3 PINs, IP addresses or biometric measurements.

1 44. The method of claim 31, further comprising the step of comparing a
2 transaction value from the transaction information to an available balance value from the
3 financial account information.

1 45. The method of claim 44, further comprising the step of presenting to
2 customers only those financial accounts with an individual or combined available fund balance
3 equal to or greater than the transaction value.

1 46. A method for facilitating payment from a customer's financial account to
2 a merchant/biller or a payment processor associated with a merchant biller, comprising the steps
3 of:

4 compiling in a memory at a payment server financial account information
5 for at least one customer, said information being received from a plurality of financial
6 institutions;

7 receiving transaction information relating to a particular customer;

8 transmitting said transaction information to the payment server and storing
9 the transaction information;

10 retrieving from the memory the financial account information for the
11 customer;

12 displaying the financial account information on an interface;

13 receiving a selection by the customer of at least one of the financial
14 accounts and storing the selection; and

15 transmitting the selected financial account(s) information either to the
16 merchant/biller or to a payment processor associated with the merchant/biller.

1 47. The method of claim 46, wherein said financial account corresponds to
2 at least one of a credit card, charge card, debit card, smart card, bank card, demand deposit
3 account, checking account, virtual payment account, virtual cash account, wire transfer networks,
4 financial electronic data interchange (FEDI), Echeck, Automated Clearing House (ACH), and
5 stored value tools.

1 48. The method of claim 46, further comprising the step of consolidating at
2 least two of said plurality of financial account information databases into a single consolidated
3 financial account information database and wherein said retrieving step includes the step of
4 searching said consolidated database.

1 49. The method of claim 46, further comprising the steps of selecting a subset
2 of one or more financial accounts from among a plurality of customer financial accounts, and
3 presenting the subset to the customer.

1 50. The method of claim 49, wherein the subset of accounts includes financial
2 accounts acceptable to the merchant/biller.

1 51. The method of claim 46, further comprising the step of dividing payment
2 for a single transaction among more than one financial account if more than one financial account
3 is selected.

1 52. The method of claim 46, further comprising the step of selecting the order
2 in which one or more financial accounts are presented to the customer before presenting the
3 financial account information to the customer.

1 53. The method of claim 46, further comprising the steps of encrypting said
2 selected customer financial account information prior to providing it to said merchant/biller, or
3 payment processor, and encrypting or truncating the financial account information before it is
4 presented to the customer.

1 54. The method of claim 46, further comprising the step of updating said
2 financial account information from at least one of said plurality of financial institutions.

1 55. The method of claim 46, further comprising the steps of determining
2 whether a customer is a registered customer; and
3 registering a customer if the customer is not yet registered.

1 56. The method of claim 55, wherein the step of registering a customer further
2 includes capturing a PIN, IP address or a biometric measurement of the customer.

1 57. The method of claim 56, wherein the biometric measurement includes
2 voice patterns, fingerprints, retina scans, or handwriting samples.

1 58. The method of claim 56, further comprising the step of comparing at least
2 one of the PIN, IP address and biometric measurement, against a respective stored database of
3 PINs, IP addresses or biometric measurements.

1 59. The method of claim 46, further comprising the step of comparing a
2 transaction value from the transaction information to an available balance value from the
3 financial account information.

1 60. The method of claim 59, further comprising the step of presenting to
2 customers only those financial accounts with an individual or combined available fund balance
3 equal to or greater than the transaction value.

1 61. The method of claim 46, wherein the interface includes a terminal, smart
2 terminal, smart box, keypad, LCD display, cardswipe device or touchpad.

1 62. The method of claim 46, wherein only those financial accounts acceptable
2 to the merchant/biller are displayed on the interface.

1 63. A method for facilitating direct bill payment by a customer, comprising
2 the steps of:

3 receiving and storing billing information from a merchant/biller or
4 merchant payment processor relating to a particular customer;

5 retrieving from a customer database financial account information for the
6 customer compiled from a plurality of financial institutions;

7 presenting to the customer a bill payment interface with one or more of
8 the customer's financial accounts;

9 receiving and storing a selection by the customer of at least one of the
10 financial accounts for payment of the bill; and

11 providing the selected financial account(s) information either to the
12 merchant/biller or to a payment processor associated with the merchant/biller.

1 64. The method of claim 63, wherein said financial account corresponds to
2 at least one of a credit card, charge card, debit card, smart card, bank card, demand deposit
3 account, checking account, virtual payment account, virtual cash account, wire transfer networks,
4 financial electronic data interchange (FEDI), Echeck, Automated Clearing House (ACH), and
5 stored value tools.

1 65. The method of claim 63, further comprising the step of consolidating at
2 least two of said plurality of financial account information databases into a single consolidated
3 financial account information database and wherein said retrieving step includes the step of
4 searching said consolidated database.

1 66. The method of claim 63, further comprising the steps of selecting a subset
2 of one or more financial accounts from among a plurality of customer financial accounts, and
3 presenting the subset to the customer.

1 67. The method of claim 66, wherein the subset of accounts includes financial
2 accounts acceptable to the merchant/biller.

1 68. The method of claim 63, further comprising the step of dividing payment
2 for a single transaction among more than one financial account if more than one financial account
3 is selected.

4 69. The method of claim 63, further comprising the step of selecting the order
5 in which one or more financial accounts are presented to the customer before presenting the
6 financial account information to the customer.

1 70. The method of claim 63, further comprising the steps of encrypting said
2 selected customer financial account information prior to providing it to said merchant/biller, or
3 payment processor, and encrypting or truncating the financial account information before it is
4 presented to the customer.

1 71. The method of claim 63, further comprising the step of updating said
2 financial account information from at least one of said plurality of financial institutions.

1 72. The method of claim 63, further comprising the steps of determining
2 whether a customer is a registered customer; and
3 registering a customer if the customer is not yet registered.

1 73. The method of claim 72, wherein the step of registering a customer further
2 includes capturing a PIN, IP address or a biometric measurement of the customer.

3 74. The method of claim 73, wherein the biometric measurement includes
4 voice patterns, fingerprints, retina scans, or handwriting samples.

1 75. The method of claim 73, further comprising the step of comparing at least
2 one of the PIN, IP address or biometric measurement, against a respective stored database of
3 PINs, IP addresses or biometric measurements.

1 76. The method of claim 63, further comprising the step of comparing a
2 transaction value from the transaction information to an available balance value from the
3 financial account information.

1 77. The method of claim 76, further comprising the step of presenting to
2 customers only those financial accounts with an individual or combined available fund balance
3 equal to or greater than the transaction value.

1 78. An apparatus for facilitating payment from a customer's financial account
2 to a merchant/biller or a payment processor associated with a merchant/biller, comprising:

3 a processor; and

4 a memory storing processing instructions for controlling the processor, the
5 processor operative with the processing instructions to:

6 compile in a memory financial account information for at least one
7 customer from a plurality of financial institutions;

8 receive and storing transaction information relating to a particular
9 customer;

10 retrieve from the memory the financial account information for the
11 customer;

12 present the financial account information to the customer;

13 receive and store a selection by the customer of at least one of the financial
14 accounts; and

15 provide the selected financial account(s) information either to the
16 merchant/biller or to a payment processor associated with the merchant/biller.

1 79. The system of claim 78, wherein said financial account corresponds to at
2 least one of a credit card, charge card, debit card, smart card, bank card, demand deposit account,
3 checking account, virtual payment account, virtual cash account, wire transfer networks, financial
4 electronic data interchange (FEDI), Echeck, Automated Clearing House (ACH), and stored value
5 tools.

1 80. The system of claim 78, wherein the processor is operative to consolidate
2 at least two of said plurality of financial account information databases into a single consolidated
3 financial account information database.

1 81. The system of claim 78, wherein the processor is operative to select a
2 subset of one or more financial accounts from among a plurality of customer financial accounts,
3 and to present the subset to the customer.

1 82. The system of claim 78, wherein the processor is operative to select a
2 subset of accounts that includes financial accounts acceptable to the merchant/biller.

1 83. The system of claim 78, wherein the processor is operative to divide a
2 payment for a single transaction among more than one financial account if more than one
3 financial account is selected.

1 84. The system of claim 78, wherein the processor is operative to select the
2 order in which one or more financial accounts are presented to the customer before presenting
3 the financial account information to the customer.

1 85. The system of claim 78, wherein the processor is operative to encrypt said
2 selected customer financial account information prior to providing it to said merchant/biller or
3 to said payment processor, and to encrypt or truncate the financial account information before
4 it is presented to the customer.

1 86. The system of claim 78, wherein the processor is operative to update said
2 financial account information from at least one of said plurality of financial institutions.

1 87. The system of claim 78, wherein the processor is operative to determine
2 whether a customer is a registered customer, and to register the customer if the customer is not
3 yet registered.

1 88. The system of claim 87, wherein the processor is operative to capture a
2 PIN, IP address or a biometric measurement of the customer as part of the registration.

1 89. The system of claim 88, wherein the biometric information includes voice
2 patterns, fingerprints, retina scans, or handwriting samples.

1 90. The system of claim 88, wherein the processor is operative to compare at
2 least one of the PIN, IP address and biometric measurement, against a respective stored database
3 of PINs, IP addresses or biometric measurements.

1 91. The system of claim 78, wherein the processor is operative to compare a
2 transaction value from the transaction information to an available balance value from the
3 financial account information.

1 92. The system of claim 91, wherein the processor is operative to present to
2 customers only those financial accounts with an individual or combined available fund balance
3 equal to or greater than the transaction value.

1 93. An apparatus for facilitating payment from a customer's financial account
2 for a bill selected from a plurality of bills presented to the customer, comprising:

3 a processor; and

4 a memory storing processing instructions for controlling the processor, the
5 processor operative with the processing instructions to:

6 compile in a memory financial account information for at least one
7 customer from a plurality of financial institutions;

8 present the customer with bill information for each of a plurality of bills;

9 receive selection information from the customer specifying a particular
10 selected bill which is to be paid;

11 retrieve from the memory the financial account information for the
12 customer;

13 present the financial account information to the customer; and

14 receive selection information from the customer specifying a particular
15 account to be used to pay the selected bill.

1 94. An apparatus for facilitating payment from a customer's financial account
2 to a merchant/biller or a payment processor associated with a merchant/biller over a computer
3 network, comprising:

4 a processor; and

5 a memory storing processing instructions for controlling the processor, the
6 processor operative with the processing instructions to:

7 compile in a memory at a payment server financial account information
8 for at least one customer, said information being received from a plurality of financial
9 institutions;

10 receive over the computer network transaction information at the payment
11 server relating to a particular customer and storing the transaction information;

12 retrieve from the memory the financial account information for the
13 customer;

14 transmit the financial account information over the computer network to
15 the customer;

16 receive over the computer network a selection by the customer of one or
17 more of the financial accounts and storing the selection; and

18 transmit the selected financial account information over the computer
19 network to said merchant/biller or a payment processor associated with the merchant/biller.

1 95. An apparatus for facilitating payment from a customer's financial account
2 to a merchant/biller or a payment processor associated with a merchant biller, comprising:
3 a processor; and
4 a memory storing processing instructions for controlling the processor, the
5 processor operative with the processing instructions to:
6 compile in a memory at a payment server financial account information
7 for at least one customer, said information being received from a plurality of financial
8 institutions;
9 receive transaction information relating to a particular customer;
10 transmit said transaction information to the payment server and storing the
11 transaction information;
12 retrieve from the memory the financial account information for the
13 customer;
14 display the financial account information on an interface;
15 receive a selection by the customer of at least one of the financial accounts
16 and storing the selection; and

17 transmit the selected financial account(s) information either to the
18 merchant/biller or to a payment processor associated with the merchant/biller.

1 96. An apparatus for facilitating direct bill payment by a customer,
2 comprising:
3 a processor; and
4 a memory storing processing instructions for controlling the processor, the
5 processor operative with the processing instructions to:
6 receive and store billing information from a merchant/biller or merchant
7 payment processor relating to a particular customer;
8 retrieve from a customer database financial account information for the
9 customer compiled from a plurality of financial institutions;
10 present to the customer a bill payment interface with one or more of the
11 customer's financial accounts;

12 receive and store a selection by the customer of at least one of the financial
13 accounts for payment of the bill; and
14 provide the selected financial account(s) information either to the
15 merchant/biller or to a payment processor associated with the merchant/biller. --.

FIG. 1

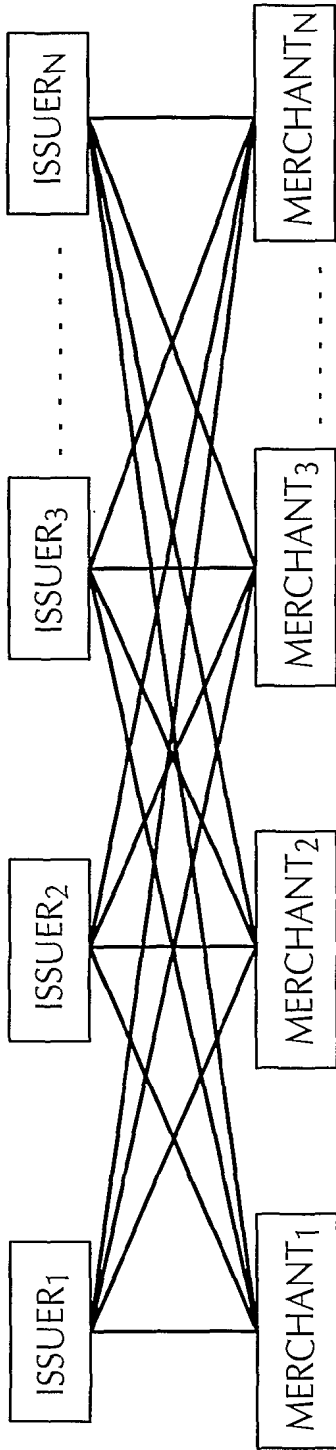


FIG. 2

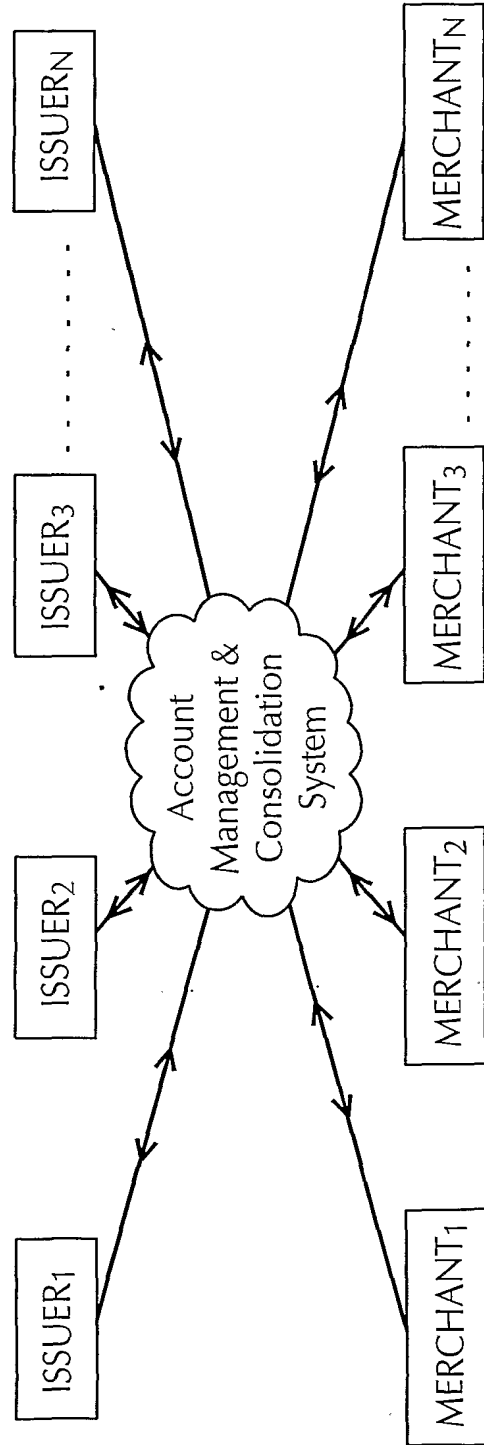
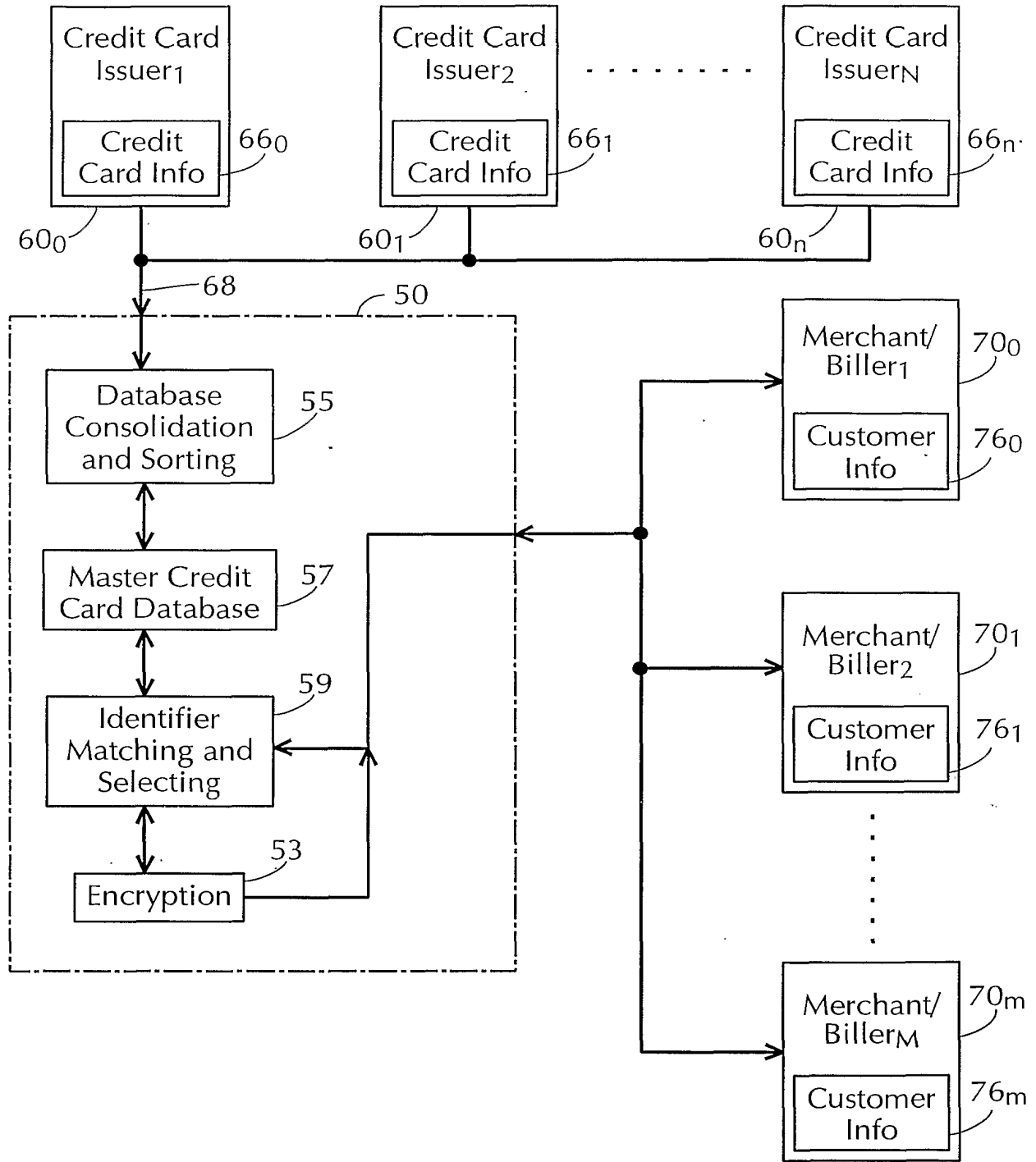


FIG. 3



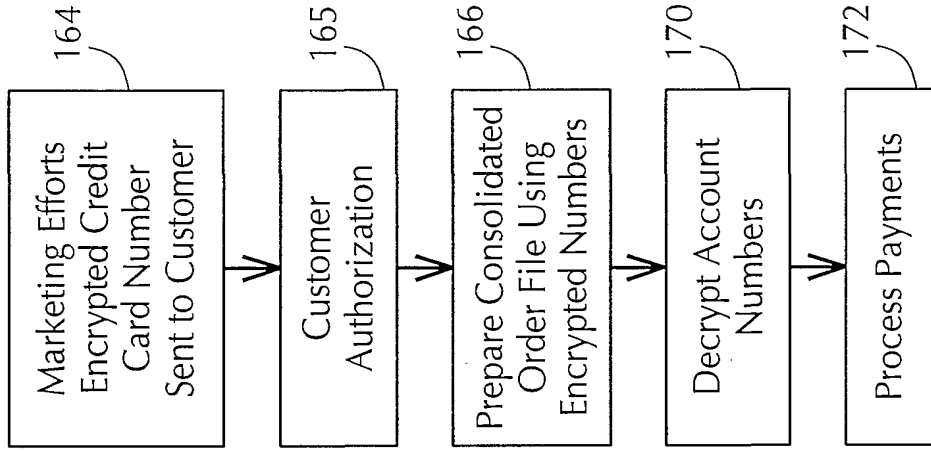


FIG. 7

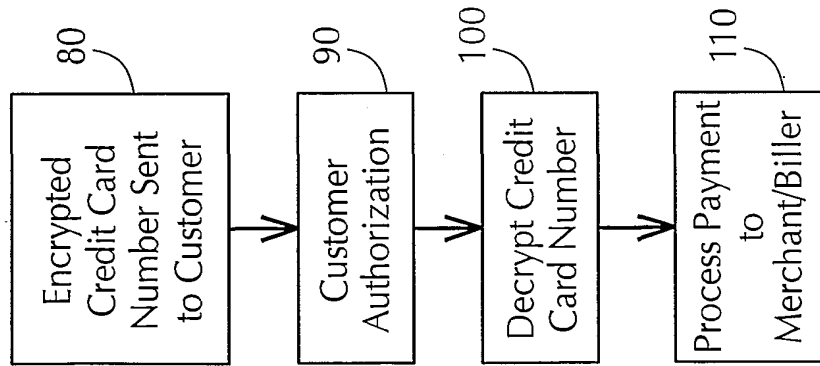


FIG. 4

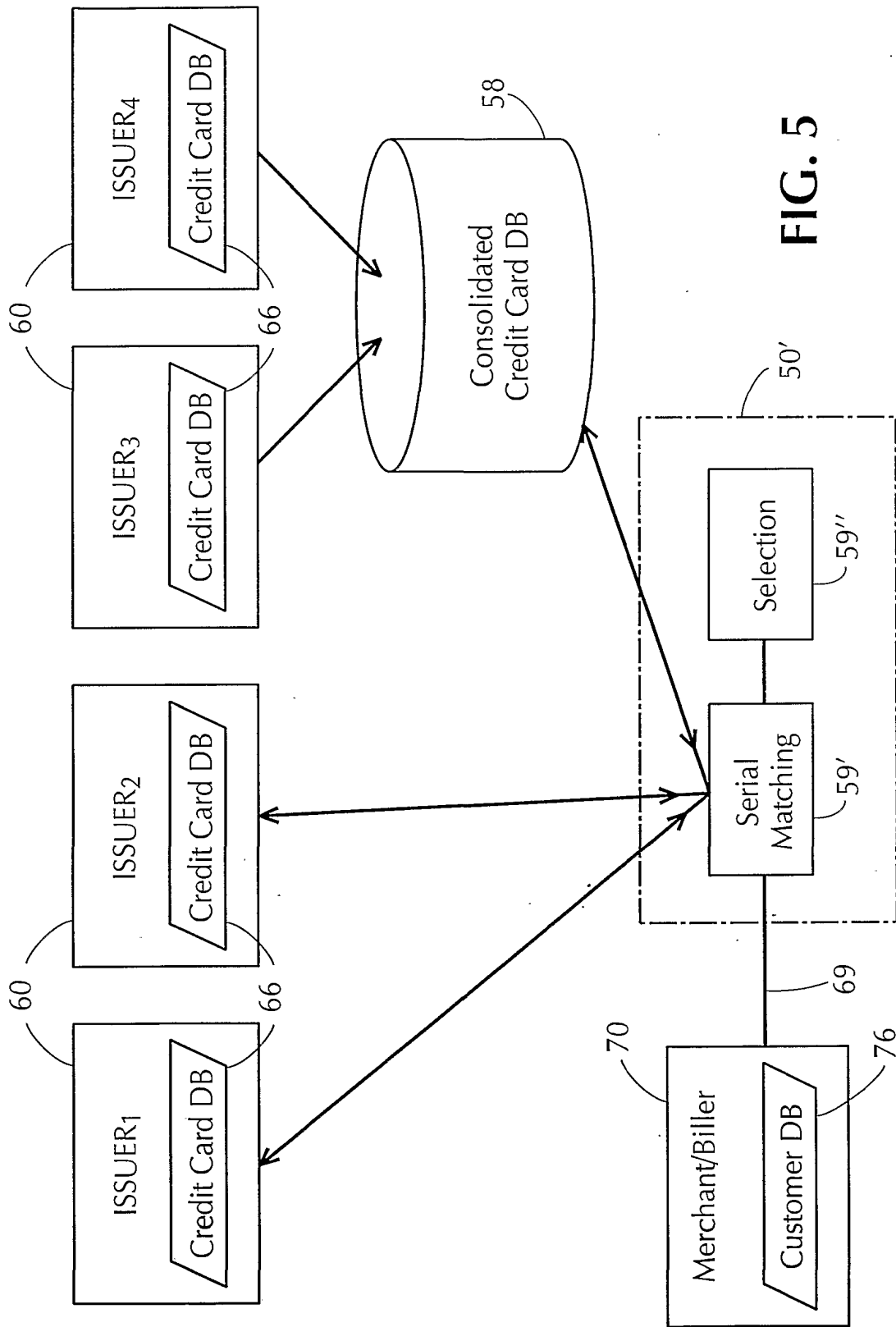


FIG. 5

FIG. 6

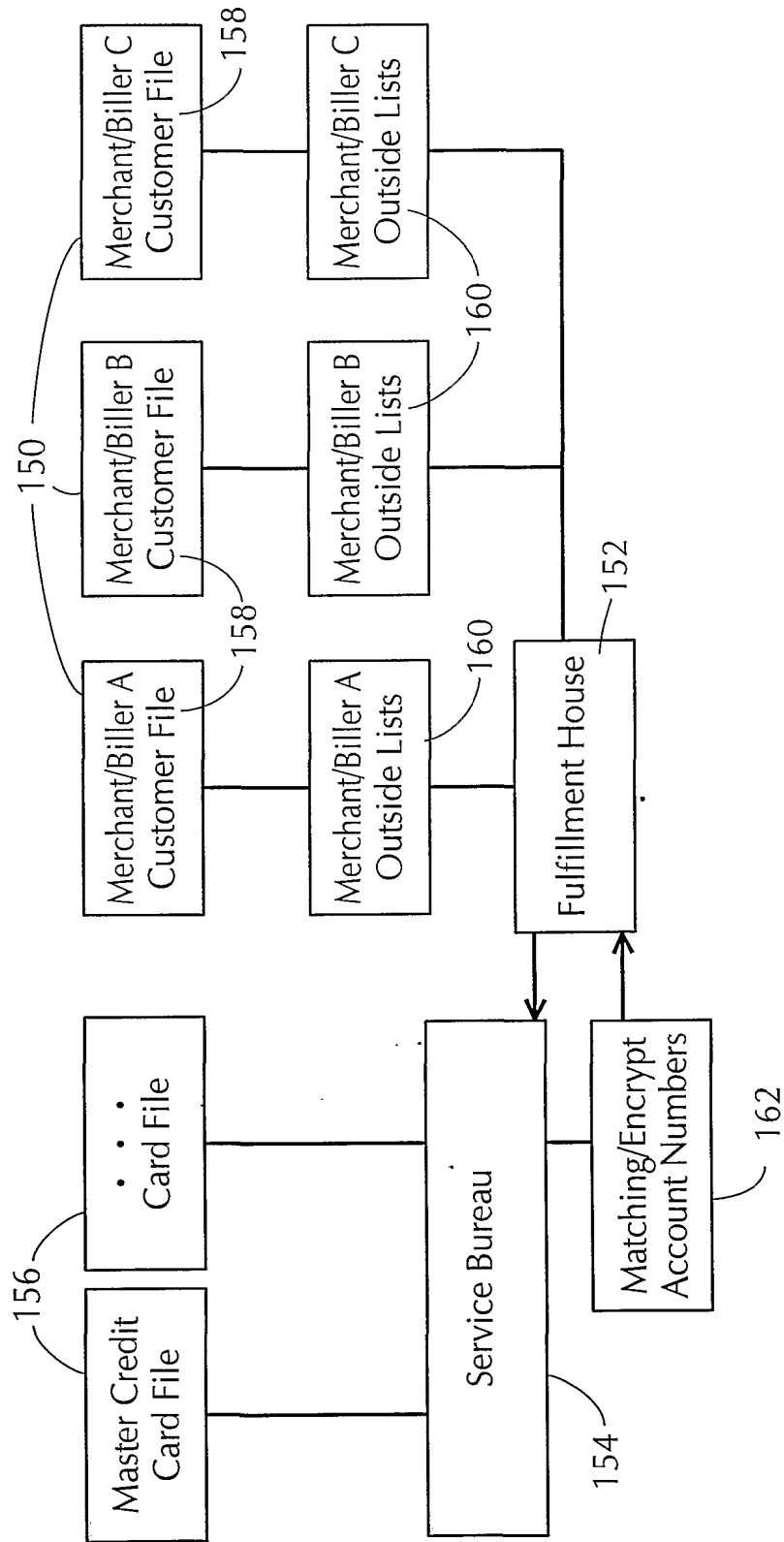
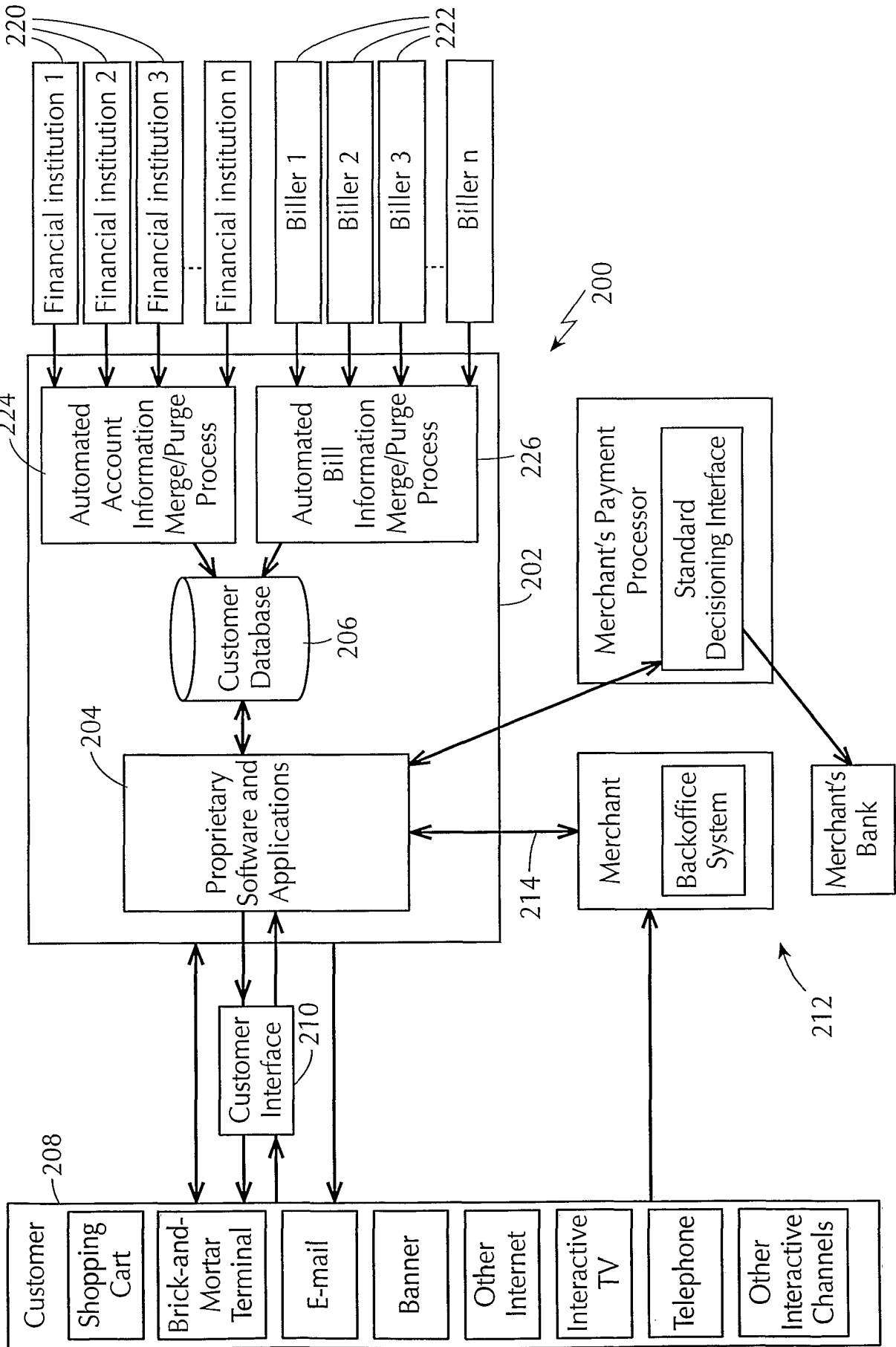


FIG. 8



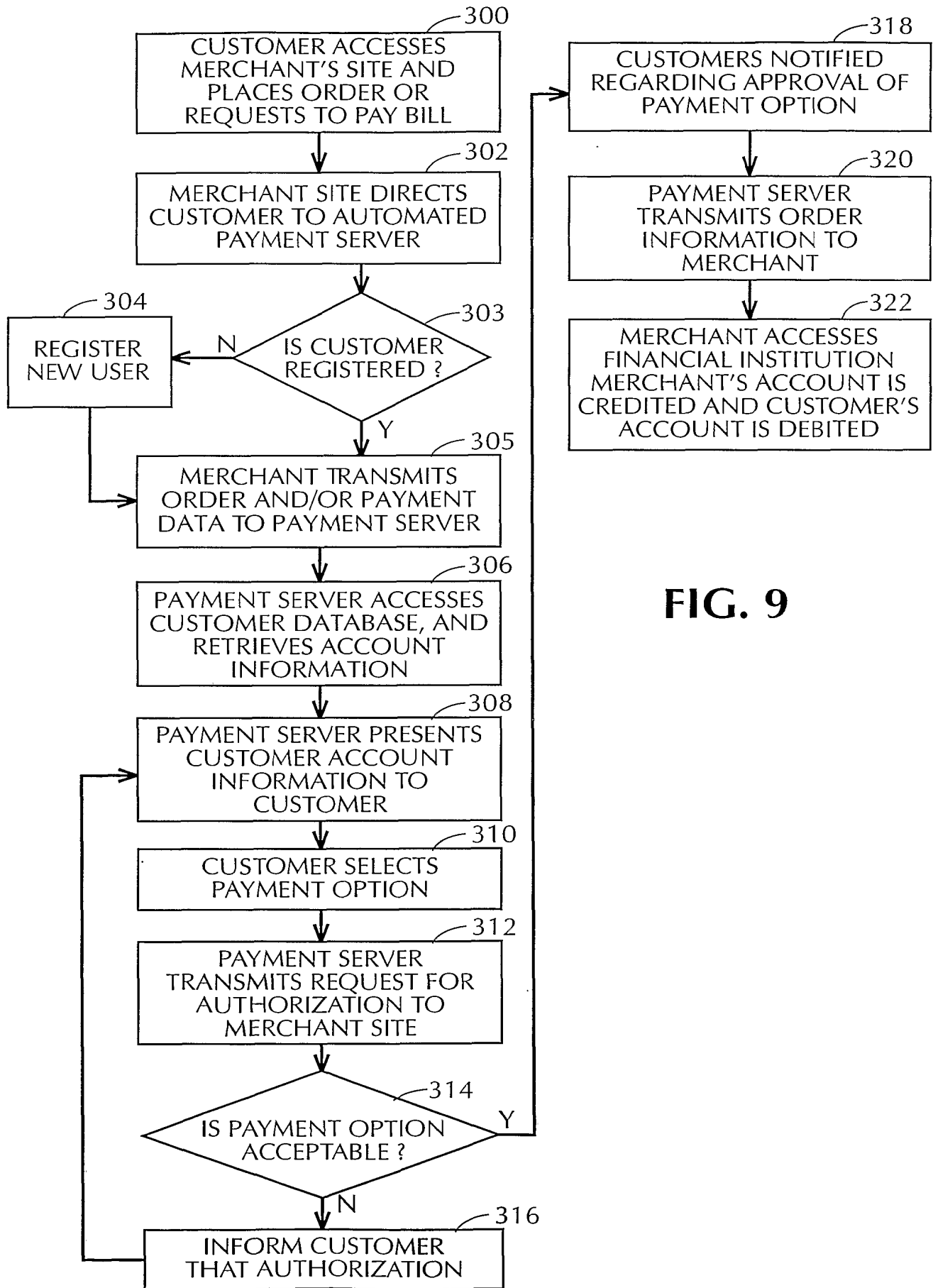


FIG. 9

FIG. 10

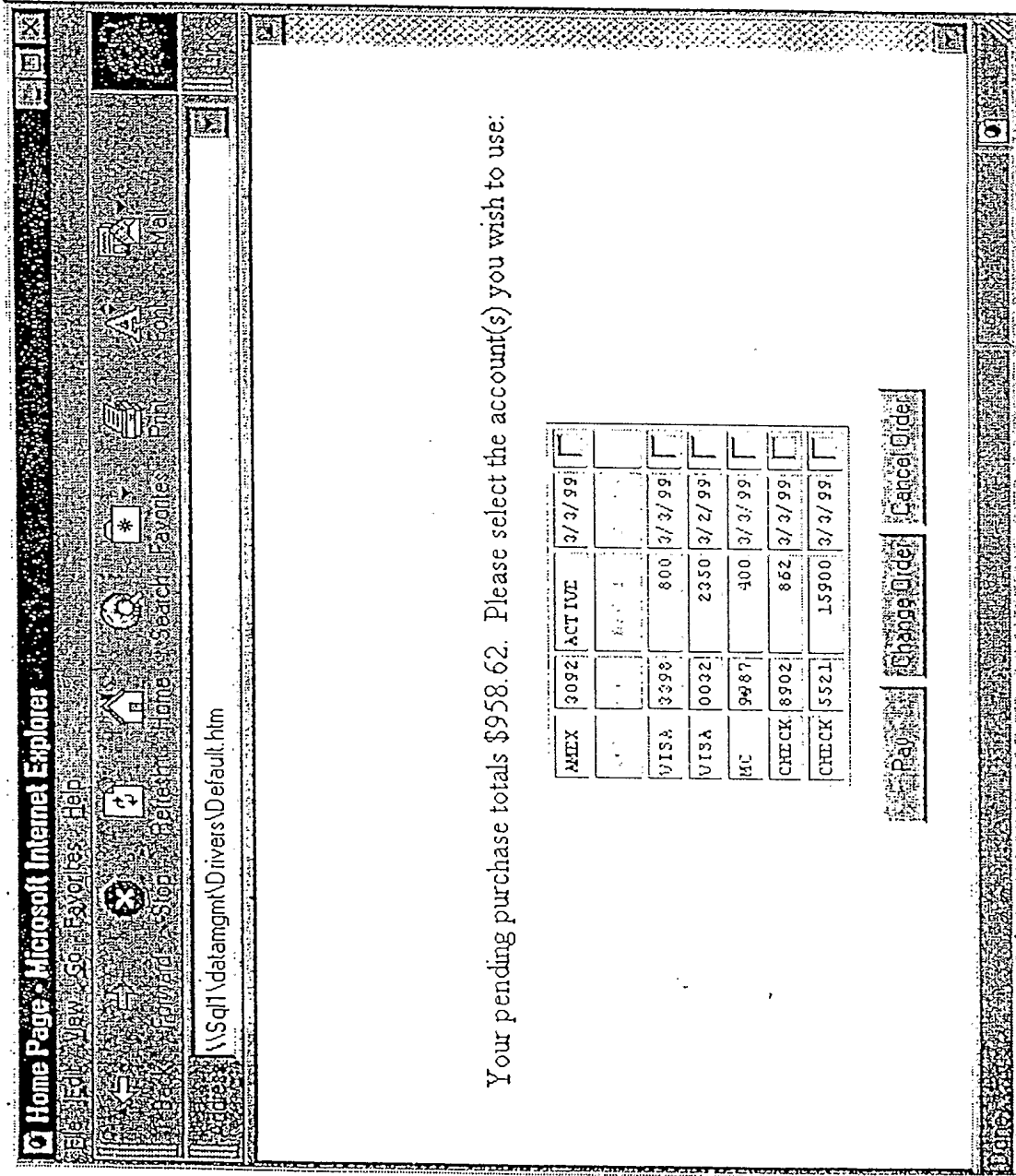
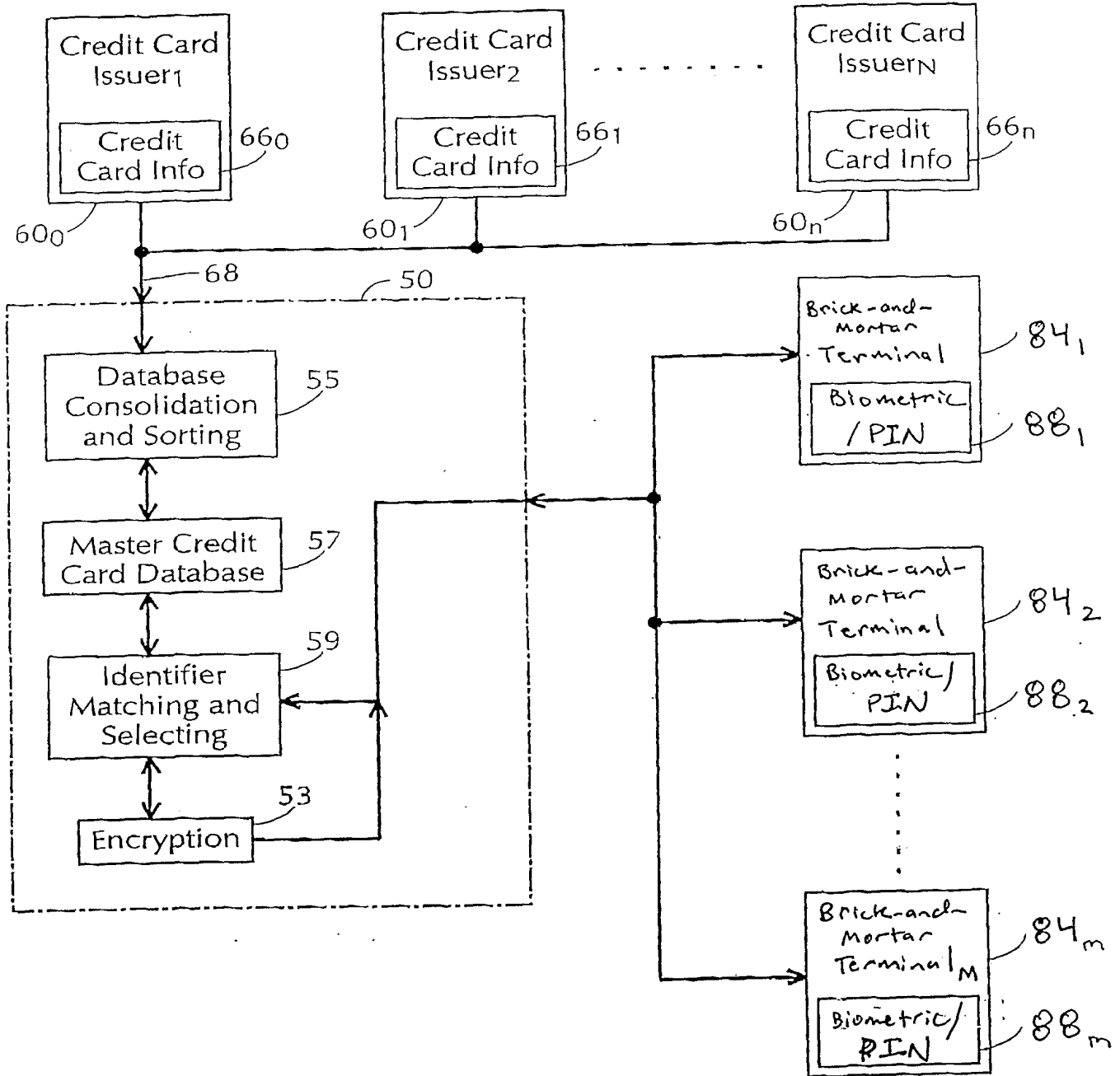


FIG. 12

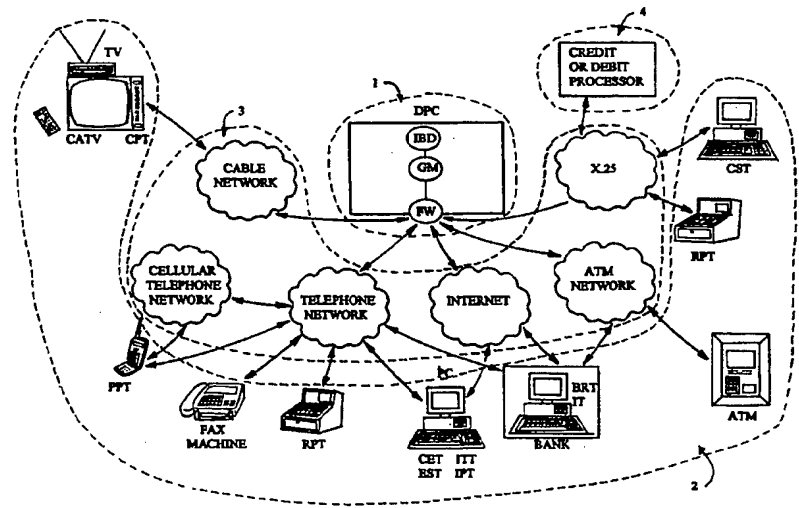




INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification ⁶ : G06K 9/00</p>	<p>A1</p>	<p>(11) International Publication Number: WO 96/36934 (43) International Publication Date: 21 November 1996 (21.11.96)</p>
<p>(21) International Application Number: PCT/US96/07185 (22) International Filing Date: 17 May 1996 (17.05.96) (30) Priority Data: 08/442,895 17 May 1995 (17.05.95) US (71) Applicant: SMART TOUCH, L.L.C. [US/US]; Suite 12, 46 Shattuck Square, Berkeley, CA 94704 (US). (72) Inventors: HOFFMAN, Ned; Suite 12, 46 Shattuck Square, Berkeley, CA 94704 (US). PARE, David, F.; Suite 12, 46 Shattuck Square, Berkeley, CA 94704 (US). LEE, Jonathan, A.; Suite 12, 46 Shattuck Square, Berkeley, CA 94704 (US). (74) Agent: KAMAREI, Ali; Suite 12, 46 Shattuck Square, Berkeley, CA 94704 (US).</p>		<p>(81) Designated States: AM, AT, AU, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, ES, FI, GB, GE, HU, JP, KE, KG, KP, KR, KZ, LK, LT, LU, LV, MD, MG, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SI, SK, TJ, TT, UA, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).</p> <p>Published <i>With international search report.</i></p>

(54) Title: TOKENLESS IDENTIFICATION SYSTEM FOR AUTHORIZATION OF ELECTRONIC TRANSACTIONS AND ELECTRONIC TRANSMISSIONS



(57) Abstract

A tokenless identification system and method are principally based on a correlative comparison of a unique biometrics sample, such as a finger print or voice recording, gathered directly from the person of an unknown user, with an authenticated biometrics sample of the same type obtained and stored previously (1). It can be networked to act as a full or partial intermediary between other independent computer systems (3), or maybe the sole computer systems carrying out all necessary executions.

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	GB	United Kingdom	MW	Malawi
AT	Austria	GE	Georgia	MX	Mexico
AU	Australia	GN	Guinea	NE	Niger
BB	Barbados	GR	Greece	NL	Netherlands
BE	Belgium	HU	Hungary	NO	Norway
BF	Burkina Faso	IE	Ireland	NZ	New Zealand
BG	Bulgaria	IT	Italy	PL	Poland
BJ	Benin	JP	Japan	PT	Portugal
BR	Brazil	KE	Kenya	RO	Romania
BY	Belarus	KG	Kyrgystan	RU	Russian Federation
CA	Canada	KP	Democratic People's Republic of Korea	SD	Sudan
CF	Central African Republic	KR	Republic of Korea	SE	Sweden
CG	Congo	KZ	Kazakhstan	SG	Singapore
CH	Switzerland	LI	Liechtenstein	SI	Slovenia
CI	Côte d'Ivoire	LK	Sri Lanka	SK	Slovakia
CM	Cameroon	LR	Liberia	SN	Senegal
CN	China	LT	Lithuania	SZ	Swaziland
CS	Czechoslovakia	LU	Luxembourg	TD	Chad
CZ	Czech Republic	LV	Larvia	TG	Togo
DE	Germany	MC	Monaco	TJ	Tajikistan
DK	Denmark	MD	Republic of Moldova	TT	Trinidad and Tobago
EE	Estonia	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	UG	Uganda
FI	Finland	MN	Mongolia	US	United States of America
FR	France	MR	Mauritania	UZ	Uzbekistan
GA	Gabon			VN	Viet Nam

**TOKENLESS IDENTIFICATION SYSTEM FOR
AUTHORIZATION OF ELECTRONIC TRANSACTIONS AND
ELECTRONIC TRANSMISSIONS**

5
By:
Ned Hoffman
David Pare
Jonathan Lee

10
Cross-Reference

The present application is a continuation-in-part of United States Patent Application Serial No. 08/345,523, filed November 28, 1994, which is incorporated herein by reference.

15
Background

20
The use of tokens and credit cards in today's financial world is pervasive. A token would be any inanimate object which confers a capability to the individual presenting the object. Remote access of every financial account is through the use of tokens or plastic cards. Whether buying groceries with debit cards or consumer goods with credit cards, at the heart of that transaction is a money transfer enabled by a token, which acts to identify an individual and the financial account he is accessing.

25
The reason for the migration from metal coins to plastic cards is simple and straightforward: access to money in this money transfer system is vastly safer and more convenient for both merchants and consumers than handling large quantities of coins and notes.

30
Unfortunately, current technology in combination with this convenient token-based money transfer system results in a system that is prone to theft and fraud.

35
As verification of user identity is based solely on data placed on the token, which can be easily reproduced and transferred between individuals, such security must rely on both the diligence and the luck of the authorized user and merchant in maintaining this information as proprietary. However, by their very nature, tokens do not have a very strong connection with the individual. Identification of the rightful owner of the token through the token is tenuous at best. This is easily

demonstrated by the fact that individuals other than the rightful owners of the tokens have been using these tokens to defraud merchants and other consumer goods suppliers.

5 The mammoth expansion of the consumer credit industry during the 1980s brought with it large profits for issuers, and newfound convenience for consumers. However, as consumer credit became easier for consumers to acquire, it also became a target for criminals. Much as the mobility of the automobile led to a rash of bank robberies in the late 1920's and early 1930's, so too did the ubiquity of consumer credit lead to vastly increased opportunities for criminals.

10 Initially, the banking industry was willing to accept a certain amount of loss due to fraud, passing the cost on to the consumer. However, as criminals became more organized, more technically adept, and as credit retail stations began to be manned by people who were more and more poorly trained in credit card security matters, the rate of increase of fraud losses skyrocketed. The staggering statistics on fraud and cost of preventive steps, has forced the credit card companies in particular, to look for other solutions to the problem.

15 Fraud losses in the credit card industry stem from many different areas due to the highly vulnerable nature of the system, but they are mainly due to either lost, stolen, or counterfeit cards. Credit cards operate without the use of a personal identification code (PIC), therefore a lost credit card can be turned into cash if the card falls into the wrong hands. While theft of a token constitutes the majority of fraud in the system, the use of counterfeit credit cards has been on the rise. Counterfeit credit cards are manufactured by a more technically sophisticated criminal by acquiring a cardholder's valid account number and then producing a counterfeit card using that valid number. The counterfeiter encodes the magnetic strip, and embosses the counterfeit plastic card with the account number. The card is then presented to merchants and charged up to the 20 rightful cardholder's account. Another form of loss is by a criminal merchant who surreptitiously obtains the cardholder's account number. Yet another type of fraud is committed by the authorized cardholder when the token is used for making purchases and thereafter a claim is made that the token was either lost or stolen. It is estimated that losses due to all types of fraud exceeds \$950 million dollars annually.

25
30
35

Generally, debit cards are used in conjunction with a personal identification code (PIC). Counterfeiting a debit card is more difficult as the criminal must acquire not only the account number, but also the PIC, and then manufacture the card as in the credit card example. However, various strategies have been used to obtain PICs from unwary cardholders; these range from Trojan horse automated teller machines, or ATMs, in shopping malls that dispense cash but record the PIC, to merchant point of sale devices that also record the PIC, to individuals with binoculars that watch cardholders enter PICs at ATMs. The subsequently manufactured counterfeit debit cards are then used in various ATM machines until the unlucky account is emptied.

The financial industry is well aware of the trends in fraud expense, and is constantly taking steps to improve the security of the card. Thus fraud and theft of token have an indirect impact on the cost to the system.

Card blanks are manufactured under very tight security. Then they are individualized with the account number, expiration date, and are then mailed to the cardholder. Manufacturing and distributing the card alone costs the industry approximately one billion dollars annually. The standard card costs the financial industry \$2 for each, but only \$0.30 of this \$2 is associated with actual manufacturing cost.

Over the last ten years, the industry has altered the tokens because of counterfeiting fraud, without any fundamental changes in the use of the credit transaction system. The remedy has been mostly administrative changes such as having customers call the issuer to activate their card. Other changes include addition of a hologram, a picture ID, or an improved signature area. These type of changes in particular, are an indication that the systems susceptibility to fraud is due to lack of true identification of the individual. It is estimated that this could double the manufacturing cost to two billion dollars annually.

In the near future, the banking industry expects to move to an even more expensive card, called a "smart card". Smart cards contain as much computing power as did some of the first home computers. Current cost projections for a first-generation smart card is estimated at approximately \$3.50, not including distribution costs, which is significantly higher than the \$0.30 plastic card blank.

5 This significant increase in cost has forced the industry to look for new ways of using the power in the smart card in addition to simple transaction authorization. It is envisioned that in addition to storing credit and debit account numbers, smart cards may also store phone numbers, frequent flyer miles, coupons obtained from stores, a transaction history, electronic cash usable at tollbooths and on public transit systems, as well as the customer's name, vital statistics, and perhaps even medical records. Clearly, the financial industry trend is to further establish use of tokens.

10 The side effect of increasing the capabilities of the smart card is centralization of functions. The flip side of increased functionality is increased vulnerability. Given the number of functions that the smart card will be performing, the loss or damage of this monster card will be excruciatingly inconvenient for the cardholder. Being without such a card will financially incapacitate the cardholder until it is replaced. Additionally, losing a card full of electronic cash will also result in a real financial loss as well. Furthermore, ability of counterfeiters to one day copy a smartcard is not addressed.

15 Unfortunately, because of the projected concentration of functions onto the smart card, the cardholder is left more vulnerable to the loss or destruction of the card itself. Thus, after spending vast sums of money, the resulting system will be more secure, but threatens to levy heavier and heavier penalties for destruction or loss of this card on the consumer.

20 The financial industry recognizes the security issues associated with smartcards, and efforts are currently underway to make each plastic card difficult to counterfeit. Billions of dollars will be spent in the next five years in attempts to make plastic ever more secure. To date, the consumer financial transaction industry has had a simple equation to balance: in order to reduce fraud, the cost of the card must increase.

25 In addition to and associated with the pervasiveness of electronic financial transactions, there is now the widespread use of electronic facsimiles, electronic mail messages and similar electronic communications. Similar to the problem of lack of proper identification of individuals for financial transactions is the problem of lack of proper identification of individuals for electronic transmissions. The ease and

30

35

speed of electronic communication, and its low cost compared to conventional mail, has made it a method of choice for communication between individuals and businesses alike. This type of communication has expanded greatly and is expected to continue to expand. However, millions of electronic messages such as facsimiles and electronic mail (or "E-mail" or "email") messages are sent without knowing whether they arrive at their true destination or whether a certain individual actually sent or received that electronic message. Furthermore, there is no way to verify the identify the individual who sent or who received an electronic message.

Recently, various attempts have been made to overcome problems inherent in the token and code security system. One major focus has been to encrypt, variablize or otherwise modify the PIC to make it more difficult for an unauthorized user to carry out more than one transaction, largely by focusing on manipulation of the PIC to make such code more fraud resistant. A variety of approaches have been suggested, such as introducing an algorithm that varies the PIC in a predictable way known only to the user, thereby requiring a different PIC code for each subsequent accessing of an account. For example, the PIC code can be varied and made specific to the calendar day or date of the access attempt. In yet another approach, a time-variable element is introduced to generate a non-predictable personal identification code that is revealed only to an authorized user at the time of access. Although more resistant to fraud than systems incorporating non-variable codes, such an approach is not virtually fraud-proof because it still relies on data that is not uniquely and irreproducibly personal to the authorized user. Furthermore, such systems further inconvenience consumers that already have trouble remembering constant codes, much less variable ones. Examples of these approaches are disclosed in United States Patents 4,837,422 to Dethloff et al.; 4,998,279 to Weiss; 5,168,520 to Weiss; 5,251,259 to Mosley; 5,239,538 to Parrillo; 5,276,314 to Martino et al.; and 5,343,529 to Goldfine et al. all of which are incorporated herein by reference.

More recently, some have turned their attention from the use of personal identification codes to the use of unique biometrics as the basis of identity verification, and ultimately computer access. In this approach, authenticated biometrics are recorded from a user of known identity and stored for future reference on a token. In every subsequent access attempt,

5 the user is required to enter physically the requested biometrics, which are
then compared to the authenticated biometrics on the token to determine if
the two match in order to verify user identity. Because the biometrics are
uniquely personal to the user and because the act of physically entering the
biometrics are virtually irreproducible, a match is putative of actual
identity, thereby decreasing the risk of fraud. Various biometrics have been
suggested, such as finger prints, hand prints, voice prints, retinal images,
handwriting samples and the like. However, because the biometrics are
generally stored in electronic (and thus reproducible) form on a token and
because the comparison and verification process is not isolated from the
hardware and software directly used by the individual attempting access, a
significant risk of fraudulent access still exists. Examples of this approach
to system security are described in United States Patents 4,821,118 to
Lafreniere; 4,993,068 to Piosenka et al.; 4,995,086 to Lilley et al.;
15 5,054,089 to Uchida et al.; 5,095,194 to Barbanell; 5,109,427 to Yang;
5,109,428 to Igaki et al.; 5,144,680 to Kobayashi et al.; 5,146,102 to
Higuchi et al.; 5,180,901 to Hiramatsu; 5,210,588 to Lee; 5,210,797 to
Usui et al.; 5,222,152 to Fishbine et al.; 5,230,025 to Fishbine et al.;
20 5,241,606 to Horie; 5,265,162 to Bush et al.; 5,321,242 to Heath, Jr.;
5,325,442 to Knapp; 5,351,303 to Willmore, all of which are incorporated
herein by reference.

As will be appreciated from the foregoing discussion, a dynamic
but unavoidable tension arises in attempting to design a security system
that is highly fraud resistant, but nevertheless easy and convenient for the
consumer to use. Unfortunately, none of the above-disclosed proposed
improvements to the token and code system adequately address, much less
attempt to balance, this tension. Such systems generally store the
authenticated biometrics in electronic form directly on the token that can
presumably be copied. Further, such systems do not adequately isolate the
identity verification process from tampering by someone attempting to gain
unauthorized access.

30 An example of token-based security system which relies on a
biometrics of a user can be found in United States Patent 5,280,527 to
Gullman et al. In Gullman's system, the user must carry and present a
credit card sized token (referred to as a biometrics security apparatus)
35 containing a microchip in which is recorded characteristics of the

authorized user's voice. In order to initiate the access procedure, the user must insert the token into a terminal such as an ATM, and then speak into the terminal to provide a biometrics input for comparison with an authenticated input stored in the microchip of the presented token. The process of identity verification is generally not isolated from potential tampering by one attempting unauthorized access. If a match is found, the remote terminal may then signal the host computer that access should be permitted, or may prompt the user for an additional code, such as a PIN (also stored on the token), before sending the necessary verification signal to the host computer.

Although Gullman's reliance of comparison of stored and input biometrics potentially reduces the risk of unauthorized access as compared to numeric codes, Gullman's use of the token as the repository for the authenticating data combined with Gullman's failure to isolate the identity verification process from the possibility of tampering greatly diminishes any improvement to fraud resistance resulting from the replacement of a numeric code with a biometrics. Further, the system remains somewhat cumbersome and inconvenient to use because it too requires the presentation of a token in order to initiate an access request.

Almost uniformly, patents that disclose token-based systems teach away from biometrics recognition without the use of tokens. Reasons cited for such teachings range from storage requirements for biometrics recognition systems to significant time lapses in identification of a large number of individuals, even for the most powerful computers.

In view of the foregoing, there has long been a need for a computer access system that is highly fraud-resistant, practical, and efficient for the user to operate and carry out electronic transactions and transmissions expeditiously.

There is also a need for a computer system that is completely tokenless and that is capable of verifying a user's personal identity, based solely upon a personal identification code and biometrics that is unique and physically personal to an authorized user, as opposed to verifying an individual's possession of any physical objects that can be freely transferred between different individuals. Such biometrics must be easily and non-intrusively obtained; must be easy and cost-effective to store and to analyze; and must not unduly invade the user's privacy rights.

5 A further need in computer access system design is user convenience. It is highly desirable for a consumer to be able to access the system spontaneously, particularly when unexpected needs arise, with a minimum of effort. In particular, there is a need for a system that greatly reduces or eliminates the need to memorize numerous or cumbersome codes, and that eliminates the need to possess, carry, and present a proprietary object in order to initiate an access request.

10 Such systems must be simple to operate, accurate and reliable. There is also a need for a computer access system that can allow a user to access multiple accounts and procure all services authorized to the user, and carry out transactions in and between all financial accounts, make point of purchase payments, receive various services, etc.

15 There is further a great need for a computer access system that affords an authorized user the ability to alert authorities that a third party is coercing the user to request access without the third party being aware that an alert has been generated. There is also a need for a system that is nevertheless able to effect, unknown to the coercing third party, temporary restrictions on the types and amounts of transactions that can be undertaken once access is granted.

20 Furthermore, the computer system must be affordable and flexible enough to be operatively compatible with existing networks having a variety of electronic transaction and transmission devices and system configurations.

25 Finally, there is a need for secured sending and receipt of electronic mail messages and electronic facsimiles, where content of the electronic message is protected from disclosure to unauthorized individuals, and the identity of the sender or recipient can be obtained with a high degree of certainty.

30 Summary of the Invention

35 The present invention satisfies these needs by providing an improved identification system for determining an individual's identity from a comparison of an individual's biometrics sample and personal identification code gathered during a bid step with biometrics sample and personal identification code for that individual gathered during a registration step and stored at a remote site wherein there is a data

5 processing center. The invention comprises a computer network host system with means for comparing the entered biometrics sample and personal identification code, and is equipped with various data bases and memory modules. Furthermore, the invention is provided with biometrics and personal identification code input apparatus and terminals for entering data to provide information for execution of the requested transactions and transmissions by the host system once the identity of the individual is determined. The invention is also provided with means for connecting the host system with the terminal and the biometrics input apparatus.

10 The computer also has means for execution of various transactions and transmission in addition to traditional storing of and modification of data. Additionally, the computer can output the evaluation of the biometrics- PIC ("personal identification code") comparison, and the determination of an identification evaluation, or status of any execution of transactions or transmissions. Furthermore, the computer system notifies and authenticates to the individual being identified that the computer system was accessed, by returning to the individual a private code which was previously selected by that individual during the registration step.

15 Preferably, the computer system is protected from electronic eavesdropping and electronic intrusion and viruses. Further, the devices used by the computer for gathering biometric samples and personal identification codes would comprise: a) at least one biometric input device for gathering biometric samples, which would have a hardware and a software component; b) at least one terminal device that is functionally partially or fully integrated with the biometric input means for input of and appending ancillary information; c) at least one data entry device for input of a personal identification code whereby this data entry device is integrated either with the biometric input device or the terminal device; and, d) a means for interconnecting the biometric input device, data entry device and the terminal. The terminal device also has at least one display device for displaying data and information. For additional security the computer system uniquely identifies the biometric input apparatus, and the counter party or merchant through a counter party or merchant identification code relating to the terminal that is connected to the biometric input device. It is also preferred that the biometric input apparatus be secured from physical and electronic tampering, and that in

20
25
30
35

case of physical breach of the device, means be employed to physically and/or electronically destroy components within the apparatus and/or erase critical data from the device's memory modules.

5 In addition, the biometric input apparatus would have a hardware component comprising: a) at least one computing module for data processing; b) erasable and non-erasable memory modules for storage of data and software; c) a biometric scanner device for input of biometric data; d) a data entry device for entering data; e) a digital communications port; f) a device for prevention of electronic eavesdropping.

10 In order to protect the integrity and confidentiality of electronic data sent between the biometric input apparatus, the terminal, and the computer network, it is preferred that the data be encrypted and sealed.

15 The host computer network is also connected to and is able to communicate with other independent computer systems, databases, facsimile machines, and other computer networks through conventional means.

20 The method of the present invention includes voluntarily identifying an individual without the use of any tokens by means of examination of at least one biometrics sample provided by that the individual and a personal identification code also provided by that individual. During a registration step, the individual is to register with the system an authenticated biometric sample, a personal identification code and a private code. Thereafter, during a bid step the biometrics sample and personal identification code of the individual is gathered and compared to the ones registered during the registration step. A match of the personal identification codes and biometrics sample will result in the positive identification of the individual. In order to authenticate to the identified individual that the real computer system was accessed, the individual's private code, which was collected at the registration step, is returned to the individual.

30 It is preferred that the method of the invention include a method for examining the biometrics samples during registration and comparing such biometrics with a collection of biometrics samples from individuals who have been designated as having previously attempted to perpetrate or who have actually perpetrated fraud upon the system.

35

In a preferred embodiment, the invention includes a method for notifying authorities of the presence of exigent circumstances or that the authorized user is under duress.

5 It is also preferred that a method of encryption and sealing of data be used to protect the data, including the digitized biometrics sample, from being revealed accidentally or unveiled from criminal elements during transmission.

10 It is also preferred that the method include steps for the individual to choose various financial accounts, and choose various modes of electronic transmissions.

It is also preferred that the method include a method for archiving of data and electronic transmissions, and retrieval of the archived data using a tracking code.

15 It is furthermore preferred that any document, such as a facsimile or an electronic mail message be uniquely checksummed using algorithm for future identification of the document.

20 Yet another method of the invention is to be able to rapidly identify an individual from an examination of his biometrics sample and personal identification code by storing several dissimilar biometrics samples from different individuals in an electronic basket that is identified by one personal identification code.

25 In one embodiment of the invention, the computer system can allow individuals to select their own personal identification code (or "PIC") from a group of PICs selected by the remote data processing center. This is performed in a method whereby once the individual's biometric is gathered, the data processing center selects several PICs at random which may be conducive to being memorized. The data processing center then conducts a comparison of the biometric gathered with those already in those PIC baskets or groups. In the event the new registrant's biometric is to similar
30 to any previously registered biometric which has been allotted to any one of those randomly selected PIC groups, then that PIC is rejected by the database for use by the new individual and an alternative PIC is selected for another such biometric comparison. Once the data processing center has generated several PIC options without a confusingly similar biometric,
35 those PICs are presented to the new registrant from which the individual may select one PIC .

In one embodiment of the invention, there is a method for rapid search of at least one first previously stored biometric sample from a first individual, using a personal identification code-basket that is capable of containing at least one algorithmically unique second biometric sample that is from at least one second individual, and which is identified by said personal identification code-basket, comprising, firstly, a storage step further comprising: a) the selection of a private code by a first individual; b) the selection of a personal identification code by said first individual; c) the entering a biometric sample from said first individual; d) locating the personal identification code-basket identified by the personal identification code selected by said first individual; e) comparison of the biometric sample taken from said first individual with any previously stored biometric samples in said selected personal identification code-basket to make sure that the biometric sample entered by said first individual is algorithmically unique from the previously stored at least one biometric sample provided by at least one second individual, and; f) storage of the entered biometric sample from said first individual in the selected personal identification code-basket if said sample is algorithmically unique from the at least one previously stored biometric sample from said at least one second individual. There is also a bid step further comprising: a) entering said selected personal identification code by said first individual, and; b) entering a biometric sample by said first individual. There is also a comparison step comprising: a) finding the personal identification code-basket that is identified by said personal identification code entered by said first individual, and; b) comparison of the entered biometric sample from said first individual with said at least one stored biometric sample from said at least one second individual in said entered personal identification code-basket for producing either a successful or failed identification result. There could also be: a) an execution step wherein a command is processed and executed to produce a determination; b) an output step wherein said identification result or said determination is externalized and displayed, and; c) a presentation step wherein on successful identification of said first individual, said private code is presented to said first individual.

According to one embodiment of the invention, the host system is positioned in series between the individual being identified and other computer networks that are to be accessed, thereby acting as an interface. It will be appreciated that in this embodiment, the user tenders an access request directly to the host computer system of the invention, which is operationally interactive with other independent secured computer systems such as VISANET. The computer system would therefore maintain authenticated biometrics data samples for all authorized users of each secured computer system that it services. These data would be cross-referenced by each authorized user. Thus, after identity verification is completed, the security system provides to the user a listing of systems that he is authorized to access, and prompts the user to select the desired network. Thereafter, the requested execution step and information regarding the transaction is forwarded to the selected independent computer network similar to the type of communications sent today between merchants and credit card companies.

In a second embodiment the host system may also carry out the functions of the other independent computer systems such as debiting or crediting a financial account. In this system, the computer system of the invention carries out the functions requested by the individual without use of external, independent computer networks.

According to a further embodiment of the invention, a means is provided for alerting predesignated authorities during an access attempt during which the user has been coerced by a third party to request access to the host computer system. In such an embodiment, an authorized user would have a number of codes, most of which would be recognized by the computer system as the standard access codes, and others which would be recognized as emergency codes. The comparison means of the computer system of the invention would be configured to accept and recognize at least one code per authorized user, and to activate the emergency alert means whenever the code entered by the user matched an emergency code. At the same time, the determination of an authorized identity for the user would result in the user being afforded access to the requested secured computer system perhaps on an access level that has been predetermined to be restricted or perhaps resulting in the display of misleading data (i.e., "false screens"), thereby preventing the coercing third party from knowing

that an emergency notification had been entered by the user. The emergency code would be entered as a part of or simultaneously with the user's personal identification code or by selecting an emergency account index during the access of the computer system. In either case, the well-being of the user requesting access might be jeopardized if the coercing party discovered that the user was attempting to notify authorities. Thus, it is critical that the access procedure continue uninterruptedly and that access be granted to an authorized user so that the coercing party believes that everything is proceeding normally. Although these features can be incorporated into the invention's host computer network, it is also possible that an independent computer network can also carry out the same or modified versions of the above-mentioned features.

The present invention is clearly advantageous over the prior art in a number of ways. First, it is extremely easy and efficient for the user, particularly where the user is accessing financial accounts, because it eliminates the need to carry and present any tokens in order to access one's accounts. The present invention eliminates all the inconveniences associated with carrying, safeguarding and locating any desired tokens. Further, because tokens are often specific to a particular computer system that further requires remembering a secret code assigned to the particular token, this invention eliminates all such tokens and thereby significantly reduces the amount of memorization and diligence increasingly required of consumers by providing access to all assets using only one personal identification code. Thus, in a single, tokenless transaction, the consumer can efficiently and securely conduct virtually any commercial exchange or electronic message, from withdrawing cash from a bank account, to authorization his agreement to the terms of a contract, to making a purchase directly from television, to paying local property taxes. The consumer is now uniquely empowered, by means of this invention, to conveniently conduct his personal and/or professional electronic transmissions and transactions at any time without dependence upon tokens which may be stolen, lost or damaged.

The invention is clearly advantageous from a convenience standpoint to retailers and financial institutions by making purchases and other financial transactions less cumbersome and more spontaneous. The paper work of financial transactions is significantly reduced as compared to

current systems, such as credit card purchase wherein separate receipts are generated for use by the credit card company, the merchant and the consumer. Such electronic transactions also save merchants and banks considerable time and expense by greatly reducing operational costs. Because the system of the invention is designed to provide a consumer with simultaneous direct access to all of his financial accounts, the need for transactions involving money, checks, commercial paper and the like will be greatly reduced, thereby reducing the cost of equipment and staff required to collect and account for such transactions. Further, the substantial manufacturing and distributing costs of issuing and reissuing credit cards, ATM cards, calling cards and the like will be eliminated, thereby providing further economic savings to merchants, banks, and ultimately to consumers. In fact, the system of the invention will likely spur economic growth since all of a consumer's electronic financial resources will be available at the mere input of his fingerprint or other biometrics.

The invention is markedly advantageous and superior to existing systems in being highly fraud resistant. As discussed above, present computer systems are inherently unreliable because they base determination of a user's identity on the physical presentation of a unique manufactured object along with, in some cases, information that the user knows. Unfortunately, both the token and information can be transferred to another, through loss, theft or by voluntary action of the authorized user. Thus, unless the loss or unintended transfer of these items is realized and reported by the authorized user, anyone possessing such items will be recognized by existing security systems as the authorized user to whom that token and information is assigned.

By contrast, the present invention virtually eliminates the risk of granting access to non-authorized users by determining user identity from an analysis of one or more of a user's unique, biometrics characteristics. Even in the very rare circumstance of coercion, where an authorized individual is coerced by a coercing party to access his accounts, the system anticipates an emergency account index, whereby the authorized user can alert authorities of the transgression without the knowledge of the coercing party.

5 The invention further enhances fraud resistance by maintaining authenticating data and carrying out the identity verification operations at a point in the system that is operationally isolated from the user requesting access, thereby preventing the user from acquiring copies of the authenticating data or from tampering with the verification process. Such a system is clearly superior to existing token-based systems wherein authenticating information, such as personal codes, is stored on and can be recovered from the token, and wherein the actual identity determination is potentially in operational contact with the user during the access process.

10 It is an object of the invention therefore to provide a computer access identification system that eliminates the need for a user to possess and present a physical object, such as a token, in order to initiate a system access request.

15 It is another object of the invention to provide a computer access identification system that is capable of verifying a user's identity, as opposed to verifying possession of proprietary objects and information.

It is yet another object of the invention to verify user identity based upon one or more unique characteristics physically personal to the user.

20 Yet another object of the invention is to provide a system of secured access that is practical, convenient, and easy use.

Still another object of the invention is to provide a system of secured access to a computer system that is highly resistant to fraudulent access attempts by non-authorized users.

25 Yet another object of the invention is to provide a computer access identification system that enables a user to notify authorities that a particular access request is being coerced by a third party without giving notice to said third party of the notification.

30 There is also a need for a computer access identification system that automatically restricts a user's transactional capabilities on the computer system according to a desired configuration provided by the user.

35 These and other advantages of the invention will become more fully apparent when the following detailed description of the invention is read in conjunction with the accompanying drawings.

Brief Description of the Drawings

FIG. 1 is a diagram of the system of the present invention;

5 FIG. 2 is a diagram of the Data Processing Center (DPC) and its internal data bases and execution modules;

FIG. 3 is a diagram of the retail point of sale terminal, the biometrics input apparatus and its components, and the interconnections between them;

10 FIG. 4 is a flow chart of the operation of the biometrics input apparatus and the terminal for generating a request packet;

FIG. 5 is a representational diagram of the request packet and the mandatory and optional data it contains;

FIG. 6 is a representational diagram of the response packet and the mandatory and optional data it contains;

15 FIG. 7 is a flow chart depicting the data encryption and sealing process at the biometrics input device;

FIG. 8 is a flow chart depicting the data decryption and counter party identification process at the DPC;

20 FIG. 9 is a flow chart depicting the data encryption and sealing process at the DPC;

FIG. 10 is a flow chart representing the registration of an individual during the registration process;

25 FIG. 11 is a flow chart representing the process of identification of the individual and returning a private code to the individual;

FIG. 12 is a flow chart of the skeleton of the processes that occur at the DPC and an execution step;

FIG. 13 is a flow chart of the emergency request and response process at the DPC;

30 FIG. 14 is a flow chart of the overall operation of retail transaction authorization execution at the DPC;

FIG. 15 is a flow chart of the overall operation of remote transaction authorization execution step at the DPC;

35 FIG. 16 is a flow chart of the overall operation of ATM account access execution at the DPC;

FIG. 17 is a flow chart of the overall operation of issuer batch modification execution at the DPC;

FIG. 18 is a flow chart of the overall operation of secure fax submit and electronic document submit execution at the DPC;

5 FIG. 19 is a flow chart of the overall operation of secure fax data and electronic document data execution at the DPC;

FIG. 20A is a representational diagram of the electronic signature request packet;

10 FIG. 20B is a representational diagram of the electronic signature response packet;

FIG. 20C is a representational diagram of the electronic signature verification request packet;

15 FIG. 20D is a representational diagram of the electronic signature verification request packet;

FIG. 21 is a flow chart of the overall operation of electronic signature execution at the DPC; and

FIG. 22 is a flow chart of the overall operation of electronic signature verification execution at the DPC.

20 Detailed Description of the Drawings

As noted, the main objective of this invention is to provide a tokenless, secure, reliable, safe, and consistent, apparatus and method, for identifying individuals for the purpose of performing financial transactions and non-financial transmissions, which can accommodate large numbers of users. It is the essence of this invention that consumers have the ability to conduct these transactions without the use of any tokens, credit cards, badges or identification cards including drivers licenses. In order to be functional it is important that the system operate at speeds required for completing financial transactions such as credit card purchases and ATM services, from multiple banks and credit accounts. The system must be secure, such that individuals records and their biometrics information remain confidential and safe, both within the computer system that identifies the individual and authorizes transactions, or during transfer of data between the computer system and remote sites with which the computer system communicates. Furthermore, the system must be reliable

in that errors in identification and authorization must not hamper or make use of the system cumbersome. Since only the use of biometrics are contemplated for identification of individuals, the system must also have security measures to either reduce access, even to the authorized user, or notify authorities in emergency cases. It is appreciated that the system must be able to handle a large number of users, and accommodate storage and transfer of large amounts of data, such as bio-characteristic information, commensurate with speeds at which financial transactions are carried on today.

Turning now to the figures, the overall configuration of the invention and its components are shown in FIG. 1. Essentially a Data Processing Center (DPC) 1 is connected to various terminals 2 through various type of communication means 3 which can be one of several types. The DPC is also connected and communicates with independent computer networks 4. The DPC contains several data bases and software execution modules as shown in FIG. 2. In a preferred embodiment of the invention, the data bases are backed up or "mirrored" for safety reasons. The Firewall Machine 5 is responsible for prevention of electronic intrusion of the system while the Gateway Machine 6 is responsible for carrying out all requests from the user, including adding, deleting and otherwise modifying all data bases. The Gateway Machine is also responsible for decryption and de-packaging of data that has arrived from the terminals using the MACM module 7, MDM module 8, and the SNM module 9. The PGL module 10, and the IML module 11 are used to locate the proper personal identification code and biometrics sample basket. FIG. 3 depicts an example of a terminal and the biometrics input device 12, which has a biometrics scanner 13, data entry means such as a key pad or PIN pad 14, and a display panel 15. The biometrics scanner can be any one of finger print scanner, voice recognition, palm print scanner, retinal scanner or the like, although the fingerprint scanner will be used as an example. The biometrics input device is further equipped with computing modules 16, device drivers, and erasable and non-erasable memory modules. The biometrics input device communicates with the terminal through preferably a serial port 17. The terminal 2 communicates through a conventional modem 18 with the DPC 1 through request packets 19 and response packets 20 using one of the interconnecting means in FIG. 1 such as cable

network, cellular telephone networks, telephone networks, Internet, ATM network, or X.25. FIG. 4 shows a representational diagram of the request packet 19 and its method of generation by the biometrics input device software. FIG. 5 and FIG. 6 show a representational diagram of the request packet and response packet with optional and mandatory data segments. Furthermore, it is shown which parts of the packets are encrypted and which ones are sealed. FIG. 7 is a block diagram of the overall process for data encryption and sealing showing the use of DUKPT key data 20 for encryption of data before appending additional data before sealing the request packet with a Message Authentication Code Key (MAC) 21. FIG. 8 and FIG. 9 show the decryption and encryption process at the DPC. FIG. 12 through 19 and 21 through 22 are block diagrams of selected examples of execution steps carried on at the DPC.

Description of the drawings, diagrams, flow charts and the description of the invention, including hardware components, software components, execution modules, data bases, connection means, the data transferred between them, and the method of the invention is described in detail as follows.

1.1. Biometric Input Apparatus (BIA)

1.1.1. Introduction

The BIA is a combination of hardware and software whose job is to gather, encode, and encrypt biometric input for use in individual identification. All actions of the BIA are directed by an outside controlling entity called a terminal, which issues commands and receives results over the BIA's serial line.

BIA hardware comes in four basic versions: standard, wireless, integrated phone/cable television (or "CATV")/fax, and ATM. Each BIA hardware variant addresses a particular need in the marketplace, and because of the differences in construction, each variant has a different level of security.

BIA software comes in seven basic versions: personal computer (or "PC"), retail, ATM, registration, internal, issuer, and integrated remote. Each software load provides a different, use-specific command set. For

instance, the registration software load does not accept requests to form retail transaction messages. Likewise, the retail software command set cannot send individual registration messages. To provide another layer of security, the DPC knows what software package is loaded into each BIA; any attempts by an BIA to send a message that it is normally not able to send is rejected, and treated as a major security violation.

The ability of the invention to detect and combat merchant-based fraud relies on the fact that the BIA's external interface is strictly limited, that the construction of the BIA makes it extremely difficult to tamper with the contents, that each BIA has its unique encryption codes that are known only to the DPC, and that each BIA is only allowed to perform operations limited to its designated function. Each biometric input means has a hardware identification code previously registered with the DPC, which makes the biometric input means uniquely identifiable to the DPC in each subsequent transmission from that biometric input device.

The BIA is constructed with the assumption that the controlling terminal is a source for fraud and deception. Terminals range from software applications running on personal computers to dedicated hardware/software systems developed for a particular use such as a retail point of sale. Regardless of the particular model, no BIA reveals unencrypted biometric information. BIA models without display means (such as LCD, LED, or quartz screens) must reveal selected information (such as individual private codes) to the terminal for display, and as a result those particular terminal-BIA combinations are considered to be less secure.

Depending on the task at hand, BIA models are either partially or fully integrated with the terminal. Partially integrated devices are physically separate from the terminal, and they include wireless and standard retail point of sale BIAs. Fully integrated devices are contained within the physical enclosure of the terminal itself, for instance, an ATM, or a telephone.

No BIA ever discloses any secret encryption codes to any external source.

1.1.2. BIA Models

Particular BIA hardware models have different configurations. They are introduced in brief here:

BIA

Standard model has computing module (i.e., multichip modules), biometric scanner (i.e., single fingerprint scanner), display means (i.e., LCD screen), communications port (i.e., serial port), data entry means (i.e., a manual data entry key board or PIC pad) encased in tamper-resistant case, and electronic detection means (i.e., RF shielding).

BIA/Wireless

Standard model, but serial line replaced with spread-spectrum wireless communications module using external antenna. Used in restaurant point of sale.

BIA/ATM

Has heavy-duty scanner and serial port, along with a multichip module. The fact that the LCD is part of the terminal and not the BIA means lower security because it must reveal the private code to the terminal. Used in ATMs.

BIA/Catv

Has light-duty scanner, otherwise like ATM. Used in telephones, CATV remotes, and fax machines. Weakest security, both because the LCD and PIC pad are part of the terminal not the BIA, and because of the low-cost nature of the market.

1.1.3. BIA Command Set Messages

Each BIA software command set provides a different set of operations. They are introduced briefly here:

BIA/ATM

Account Access

BIA/Catv

Remote Transaction Authorization

BIA/Fax

Secure Fax Submit

Secure Fax Data

Secure Fax Tracking

Secure Fax Retrieve

Secure Fax Reject

Secure Fax Archive

Secure Fax Contract Accept

Secure Fax Contract Reject

Electronic Document Archive Retrieve

BIA/Internal

Individual Identification

BIA/Issuer

Issuer Batch

BIA/PC

Electronic Document Submit

Electronic Document Data

Electronic Document Tracking

Electronic Document Retrieve

Electronic Document Reject

Electronic Document Archive

Electronic Document Archive Retrieve

Electronic Signature Submission

Electronic Signature Check

Remote Transaction Authorization

Network Credential

Secured Connection

BIA/Registration

Individual Identification

Biometric Registration

5

BIA/Retail

Transaction Authorization

1.1.4. BIA Hardware: Standard Model

10

The Standard BIA hardware is a multichip module combined with a single-print scanner, an LCD screen, a serial port, and a PIC pad encased in a hard tamper-resistant case that makes attempts to penetrate obvious while also providing RF shielding for the contents.

15

The following components are amalgamated into a multichip module, called the BIA Multichip Module (a process for encapsulating several processors in one physical shell, well known in the industry), constructed to protect the communications pathways between the devices from easy wiretapping.

20

- Serial processor
- PIC pad processor
- LCD screen processor
- CCD scanner A/D processor
- High-speed DSP processor containing both flash and mask ROM
- General purpose microprocessor
- Standard RAM
- EEPROM

25

30

The following software packages and data are stored in mask ROM. Mask ROM is cheaper than other types of read only memory, but it is easily reverse engineered, and is not electronically erasable. As such we only place the noncritical commonly available code here. (Mask ROM is well known in the industry).

35

- MAC calculation library
- DUKPT Key Management library
- DES (with CBC) Encryption library
- Base-64 (8-bit to printable ASCII) converter library
- Public Key Encryption library
- Embedded Operating System
- Serial line device driver
- LCD device driver
- PIC pad device driver
- Scanner device driver
- Unique hardware identification code
- Multi-Language profiles

The following standard data and software packages are stored in flash ROM. Flash ROM is more expensive, but it is much more difficult to reverse engineer, and most importantly, it is electronically erasable. All of the more critical information is stored here. Flash ROM is used in an attempt to increase the difficulty of duplicating an BIA. (Flash ROM is well known in the industry).

- Unique DUKPT Future Key Table
- Unique 112-bit MAC Key
- DSP biometric quality determination algorithm
- DSP biometric encoding algorithm
- Random number generator algorithm
- Command function table

The message sequence number, incremented each time a message is sent from the BIA, is stored in the EEPROM. EEPROM can be erased many times, but is also nonvolatile — its contents remain valid across power interruptions. (EEPROM is well known in the industry).

The following data is stored in RAM. RAM is temporary in nature, and is lost whenever power is lost.

- Encoded Biometric Register
- PIC Register

- Account Index Code Register
- Title Index Code Register
- Amount Register
- Document Name Register
- 5 • PIC-Block Key
- Message Key
- Response Key
- Shared Session Key
- Private Session Key
- 10 • 8 General Registers
- stack and heap space

Each multichip module contains a "write-once" memory location that is irreversibly set following the initialization of the flash ROM. Whenever an attempt is made to download software to the flash ROM, this memory location is checked; if it is already been set, then the BIA refuses to load. This way, critical software and data keys may only be downloaded once into the device, at the time of manufacture.

All registers and keys are explicitly zeroed when a transaction is canceled. Once a transaction is completed, registers are cleared as well. Once a "form message" command is executed, biometric, PIC, and account index code registers are also cleared, along with any encryption keys that aren't required for subsequent use.

It is important that the software not keep copies of registers or keys in stack variables (known in the industry).

The following associated hardware components comprise the standard BIA hardware module.

- BIA Multichip module
- CCD single-print scanner
- capacitance detector plate (known in the industry)
- lighted PIC keypad
- 2-line 40-column LCD screen
- 35 • RF shielding
- tamper-resistant case

- serial connection (up to 57.6kb)
- breach detection hardware (known in the industry)
- optional thermite charge attached to Multichip module (known in the industry)

5
10
All temporary storage and internal hardware and software used to calculate these values are secured, which means they resist any attempts to determine their current values, or their means of functioning. This feature is essential for the security of the invention, just as it is critical that the "wiretapping" of an BIA and specifically the gathering of a Biometric-PIC Block for fraudulent means is made as difficult as possible.

The multichip module and the components are, where practical, physically connected to each other without exposed wiring being present.

15
20
The enclosure protecting the electronic components of the BIA is welded shut during manufacture; it cannot be opened under any circumstances without significant damage to the case. Upon detecting any opening (or damage) of the enclosure, the BIA performs an emergency electronic zero of any and all keys residing in flash ROM, followed by all of the software libraries. Specific breach detection methods are kept confidential and proprietary.

In addition to protecting the contents, the case also shields the internal operations from RF signal detectors.

25
Supersecure versions of the BIA exist whereby breach detection methods are connected to a mechanism that physically destroys the multichip module as well as the detection methods themselves.

1.1.5. BIA Hardware: Wireless Model

30
The Wireless version of BIA hardware is identical to the Standard model in construction, except that it exports a spread-spectrum wireless communications module using an external antenna instead of an external serial port.

This version is designed to be used in restaurants, where transactions are authorized at the customer's convenience.

In the following descriptions, items which are added to the standard set are signified by the + character, while items that are removed from the standard set are signified by the – character.

5

Multichip Module:

- Document Name Register
- Shared Session Key
- Private Session Key
- Message Key

10

Components:

- Serial port
- + External antenna
- + Spread-spectrum wireless serial module (known in the industry)

15

1.1.6. BIA Hardware: ATM Model

The ATM version of BIA hardware is a multichip module combined with a heavy-duty single-print scanner and a serial port. The components are encased in a tamper-resistant case that makes attempts to penetrate obvious while also providing RF shielding for the contents.

20

This version is designed to be retrofitted into ATM locations. As such, the scanner pad is a heavy-duty sensor pad, and the entire construction makes use of the existing screens and keypads present in the ATM itself.

25

In the following descriptions, items which are added to the standard set are signified by the + character, while items that are removed from the standard set are signified by the – character.

30

Multichip Module:

- Amount Register
- Document Name Register
- Shared Session Key
- Private Session Key
- Message Key

35

Components:

- lighted PIC keypad
- 2-line 40-column LCD screen

5 Note that since the ATM has no LCD screen or PIC keypad, it really has no need of those device drivers in the mask ROM.

1.1.7. BIA Hardware: Phone/CATV Model

10 The Phone/CATV version of BIA hardware is a multichip module combined with a single-print scanner and a serial port. The module is physically attached to the scanner, and the whole is encased in plastic in order to make tampering more difficult. Some amount of RF shielding is provided for the components.

15 This version is designed to be integrated with telephones, television remote controls, and fax machines. As a result, it makes use of the existing keypads and LCD or television screens to enter or display values. It also uses the communication facilities of the host terminal. For example, the fax machine uses the built-in fax modem and the television remote uses the CATV cable network.

20 This hardware model is (in comparison with other models) relatively insecure, as it is intended that these devices cost as little as possible, be lightweight, and integrate easily with existing low-cost devices.

25 Of course, higher-security versions with more complete enclosures are possible and encouraged.

30 In the following descriptions, items which are added to the standard set are signified by the + character, while items that are removed from the standard set are signified by the - character.

Multichip Module:

- Document Name Register
- Shared Session Key
- Private Session Key
- Message Key

Components:

- lighted PIC keypad
- 2-line 40-column LCD screen

5

1.2. BIA Software**1.2.1. BIA Software Command Interface:**

10

The external interface to the BIA is much like a standard modem; commands are sent to it from a controlling terminal using the external serial line. When a command completes, a response code is sent from the BIA to the terminal.

15

Each BIA software load supports a different set of operations. For instance, a retail load supports only transaction authorizations, while a registration load supports individual identification and biometric registration.

20

All BIA data fields are in printable ASCII, with fields separated by field separator (or "fs") control character, and records separated by newlines. Encrypted fields are binary converted to 64-bit ASCII using the base-64 conversion library (all known in the industry).

Some commands are not available in some configurations. For instance, the ATM BIA cannot "Get PIC", since there is no attached PIC pad. Instead, the ATM BIA supports a "Set PIC" command.

25

Response Codes:**Out of time:**

30

The time allotted for the command has expired. A message to that effect will be displayed on the LCD screen, if available. When time expires for a given command, the BIA acts as if the cancel button was pushed.

Canceled:

35

The "cancel" button has been pushed, and the entire operation has been canceled. This has the side effect of clearing all information

which was gathered. A message to that effect will be displayed on the LCD screen, if available.

Ok:

The command was successful.

Other:

Each command may have specific other response codes which are valid only for it. These response codes will generally have text accompanying the code, which will be displayed on the LCD screen if it is available.

Message:

This indicates that the command is ongoing, but that the BIA wants to send a message to the terminal with an interim result message. The result is also displayed on the LCD, if available. This facility is used for prompts, as well as status messages.

Commands:

In the argument list of the commands below, the < > characters surround individual arguments, [] characters surround optional arguments, and the | character indicates that a given argument may be comprised of one of the choices presented.

Set Language <language-name>

This command selects from one of a number of different languages encoded within the BIA for prompting for user input.

Get Biometric <time> [primary|secondary]

This command requests the BIA to activate its scanner to get biometric input from the individual, storing it into the Encoded Biometric Register.

First, the message "Please place finger on lighted panel" is displayed on the LCD panel and returned to the terminal. The scanner pad is illuminated, prompting the individual to enter his biometric.

A <time> value of zero means that there is no limit to the time for biometric scan input.

When in scanning mode, a fingerprint scan is taken and given a preliminary analysis by the print quality algorithm. If the scan is not good enough, the BIA continues to take new scans until <time> seconds pass. As time passes and snapshots of the print are taken and analyzed, messages are posted to the LCD screen and sent to the terminal based on the problems detected by the print quality software. If no print of appropriate quality is forthcoming, the BIA returns an error code of time expired, displaying a message to that effect on the LCD.

Once the print quality algorithm affirms the quality of the print scan, the print's minutiae are then extracted by the print encoding algorithm. Only a subset of the minutiae are selected at random, with care taken to retain enough sufficient for identification. These minutiae are then ordered randomly, and are placed in the Encoded Biometric Register. Then the BIA responds with the success result code.

If the [primary|secondary] is specified (only available in the biometric registration command set) then the entire minutiae set is selected, not just the smaller subset. Likewise, primary/secondary biometric selection ends up placing the encoded biometric into the appropriate register.

Whether or not the operation succeeds, as soon as scanning has terminated, the light indicating that scanning is in progress is turned off.

It is very important that the same biometric input yields different encodings, so as to complicate the task of anyone attempting to discover the encryption codes of a captured BIA. This is accomplished by the selection of a random subset and random ordering of the encoded biometric.

Get PIC <time>

This command requests the BIA to fill the PIC Register by reading from the keypad.

First, the message "Please enter your PIC, then press <enter>" is displayed on the LCD display and sent to the terminal, the appropriate keypad lights are turned on, and then keypad scanning begins.

Scanning terminates when either <time> number of seconds runs out, or when the individual hits the "enter" key.

Note that the individual digits of the PIC are not displayed on the LCD panel, but for each digit the individual types, a star "*" appears to give the individual feedback. When the "correction" key is pressed, the last digit entered is erased, allowing the individual to fix input mistakes.

When PIC input terminates, the keypad lights turns off.

If successful, the command returns OK.

Get Account Index Code <time>

First, the message "Now enter your account index code, then press <enter>" is displayed on the LCD and sent to the terminal. This prompts the individual to enter his account index code. When each key is pressed, that value appears on the LCD panel. The correction button can be pressed to erase one of the values. When the "enter" button is pressed, the Account index code register is set.

During input, the appropriate keypad keys are lit, and when input is concluded, the keypad lights are turned off.

If successful, the command returns OK.

Get Title Index Code <time>

First, the message "Please enter your title index code, then press <enter>" is displayed on the LCD and sent to the terminal. This prompts the individual to enter his title index code. When each key is pressed, that value appears on the LCD panel. The correction button can be pressed to erase one of the values. When the "enter" button is pressed, the Title Index Code register is set.

During input, the appropriate keypad keys are lit, and when input is concluded, the keypad lights are turned off.

If successful, the command returns OK.

Validate Amount <amount> <time>

The Validate Amount command sends the message "Amount <amount> OK?" to the terminal, and displays it on the LCD screen. If the individual confirms the amount by hitting the "yes" (or enter) button, the Amount Register is set to <amount>. The <amount> value must be a valid number,

with no control characters or spaces, etc. During prompting, the yes, no, and cancel buttons are lit. Once prompting is complete, all the lights are turned off.

If the individual enters "no", then the transaction is canceled.

5

Enter Amount <time>

The Enter Amount command sends the message "Enter amount" to the terminal, and also displays it on the LCD screen as well. The individual must then enter the dollar amount himself. Each character entered is displayed on the LCD screen. All appropriate buttons are lit. If the enter button is hit, the Amount Register is set to be the value entered on the keyboard. Once entry is complete, all the lights are turned off.

10

Validate Document <name> <time>

The Validate Document command sends the message "Document <name> OK?" to the terminal, and displays it on the LCD screen as well. If the individual confirms the document by hitting the "yes" (or enter) button, the Document Name Register is set to <name>. The <name> must be printable ASCII, with no control characters, and no leading or trailing spaces. During prompting, the yes, no, and cancel buttons are lit. Once prompting is complete, all the lights are turned off.

15

20

If the individual enters "no", the transaction is canceled.

Assign Register <register> <text>

The assign register command sets the designated General <register> to have the value <text>. This is used to set information such as the merchant code, the product information, and so on.

25

Get Message Key

The Get Message Key command causes the BIA to generate a 56-bit random key to be used by the controlling hardware to encrypt any message body that the controlling device wishes to add to the message. That generated key is returned by the BIA in hexadecimal format (known in the industry). The message key are then added to the biometric-PIC block.

30

35

Form Message <type=identification|transaction|account access...>

The form message command instructs the BIA to output a message containing all the information it has gathered. It also checks to make sure that all the registers appropriate to that specific message <type> have been set. If all required registers are not set, the BIA returns with an error. The specific command set software will determine which messages can be formed by that BIA model; all others will be rejected.

Each message includes a transmission code consisting of the BIA's unique hardware identification code and an incrementing sequence number. The transmission code allows the DPC to identify the sending BIA and to detect resubmission attacks.

The BIA uses the DUKPT key management system to select the biometric-PIC block encryption 56-bit DES key from the Future Key Table. This key is then used to encrypt the Biometric-PIC Block using cipher block chaining (CBC). In addition, a response DES key is also generated randomly, and is used by the DPC to encrypt the portions of the response that need to be encrypted.

Note: splitting the response key from the biometric-PIC block key is very important, since each encryption key must be used only within the context of its own responsibilities. That way, if someone were to break the key encoding the private code, it would not result in the disclosure of the biometric-PIC.

The Biometric-PIC block consists of the following fields:

300-byte authorization biometric

4-12 digit PIC

56-bit response key

[optional 56-bit message key]

Note that the message key is only present if the controlling terminal has requested a message key for this message. It is up to the controlling terminal to encrypt any message body attached to the transaction authorization request using the message key.

Once all encryption is complete, the BIA outputs the body of the appropriate request message (such as a Transaction Authorization

Request message), terminated by and protected with the Message Authentication Code (MAC).

5 The MAC field is calculated using the BIA's secret 112-bit DES MAC key, and covers all message fields from first to last. The MAC assures the DPC that nothing in the message has changed effectively sealing the message, while still allowing the plaintext fields to be inspected by the controlling terminal.

10 When the Form Message command is done, the BIA sends the message "I'm talking to DPC Central" to the terminal as well as displaying it on the LCD screen, indicating that work is proceeding on the request.

The command returns OK in addition to returning the entire formed message upon completion of the command.

Show Response <encrypted response> <time>

15 The Show Response command instructs the BIA to use its current Response Key to decrypt the private code from the system.

20 After decryption, a chime sounds, and the private code is displayed on the LCD screen for <time> seconds. At no time does this command transmit the decrypted private code to the controlling terminal.

Validate Private <encrypted validation> <time>

25 This command is used by a terminal during a secure network communications session to ask the individual to validate a message from an outside source. The message comes encrypted and in two parts: the challenge, and the response.

30 Upon receipt of a Validate Private command, the BIA displays the text of the challenge message as in "OK <challenge>?" on the LCD screen, but does not send this to the terminal. When the individual validates the challenge, the response is encrypted by the BIA using the Private Session Key, and then returned to the terminal along with the OK response code. If the individual does not validate the challenge, then the BIA returns with a "failed" response code, along with the text "transaction canceled at your request," which is also displayed on the LCD screen.

35 Note that the terminal is never allowed to see the plaintext of either the challenge or the response.

Reset

The Reset command instructs the BIA to clear all temporary registers, the LCD screen, all temporary Key registers, and to turn off all keypad lights that may be on.

5

Set PIC <value>

This command assigns the BIA's PIC Register to be <value>.

Note that allowing a non-secured device to provide the PIC is a potential security problem, because non-secured devices are much more vulnerable to wiretapping or replacement.

10

Set Account index code <value>

This command assigns the BIA's Account index code Register to be <value>.

15

Note that allowing a non-secured device to provide the account index code is a potential security problem, because non-secured devices are much more vulnerable to wiretapping or replacement.

Set Title Index Code <value>

This command assigns the BIA's Title Index Code Register to be <value>.

20

Note that allowing a non-secured device to provide the Title Index Code is a potential security problem, because non-secured devices are much more vulnerable to wiretapping or replacement.

25

Set Amount <value>

This command assigns the BIA's Amount Register to be <value>.

30

Decrypt Response <encrypted response message>

The Decrypt Response command instructs the BIA to use it's current Response Key to decrypt the encrypted portion of the response message. Once decrypted, the response is returned to the controlling device, presumably for display on the ATM terminal's LED screen.

35

Note that providing this decryption ability is a security problem, as once the plaintext leaves the BIA, the terminal has the ability to do with it what it will.

1.2.2. BIA Software: Support Libraries

The BIA software is supported by several different software libraries. Some of them are standard, generally available libraries, but some have special requirements in the context of the BIA.

1.2.2.1. Random Number Generator

Since the BIA is constantly selecting random DES keys for use in the message body and message response encryption, it is important that the keys selected be unpredictable keys. If the random number generator is based on time of day, or on some other externally-predictable mechanism, then the encryption keys will be much more easily guessed by an adversary that happens to know the algorithm. In order to assure the security of the encryption techniques used in the BIA, it is assumed that both the random number generator algorithm as well as the encryption algorithms are both publicly known.

A standard random number algorithm for generating DES keys is defined in ANSI X9.17, appendix C (known in the industry).

1.2.2.2. DSP Biometric Encoding Algorithms

The biometric encoding algorithm is a proprietary algorithm for locating the minutiae that are formed by ridge endings and bifurcations on human fingertips. A complete list of minutiae is stored in the DPC as a reference, while only a partial list is required by the algorithm when performing a comparison between an identification candidate and a registered individual.

During both biometric registration as well as identification, the encoding algorithm ensures that enough minutiae are found before ending the biometric input step.

1.2.2.3. Operating System and Device Drivers

5 The BIA is a realtime computing environment, and as such requires a realtime embedded operating system to run it. The operating system is responsible for taking interrupts from devices and scheduling tasks.

10 Each device driver is responsible for the interface between the operating system and the specific hardware, such as the PIC pad device driver, or the CCD Scanner device driver. Hardware is the source for events such as "PIC pad key pressed", or "CCD Scanner scan complete". The device driver handles such interrupts, interprets the events, and then takes action on the events.

1.2.2.4. DES Encryption Library

15 There are any number of DES implementations publicly available. DES implementations provide a secret key-based encryption from plaintext to ciphertext, and decryption from ciphertext to plaintext, using 56-bit secret keys.

1.2.2.5. Public Key Encryption Library

20 Public Key encryption support libraries are available from Public Key Partners, holders of the RSA public key patent (known in the industry). Public Key cryptosystems are asymmetric encryption systems that allow communication to take place without requiring a costly exchange of secret keys. To use a public key encryption system, a public key is used to encrypt a DES key, and then the DES key is used to encrypt a message. The BIA uses public key cryptosystems to provide for the secure exchange of secret keys.

25 Unfortunately, public key systems are significantly less well tested than secret-key systems, and as such there is an overall lower level of confidence in such algorithms. As a result, the invention uses public key cryptography for communications security and short-lived credential exchange, and not long-term storage of secrets. Both the end-user individual and the bank are identified by the DPC to create the network

credential. The network credential includes the end-user individual's identification as well as the context of the connection (i.e., the TCP/IP source and destination ports).

5 1.2.2.6. DUKPT Key Management Library

The derived unique key per transaction key (DUKPT) management library is used to create future DES keys given an initial key and a message sequence number. Future keys are stored in a Future Key Table. Once used, a given key is cleared from the table. Initial keys are only used to generate the initial future key table. Therefore the initial key is not stored by the BIA

10 The use of DUKPT is designed to create a key management mechanism that provided a different DES key for each transaction, without leaving behind the trace of the initial key. The implications of this are that even successful capture and dissection of a given future key table does not reveal messages that were previously sent, a very important goal when the effective lifetime of the information transmitted is decades. DUKPT is fully specified in ANSI X9.24 (known in the industry).

15 DUKPT was originally developed to support PIC encryption mechanisms for debit card transactions. In this environment, it was critical to protect all transactions. An assumption is made that a criminal records encrypted transactions for a six month period, and then captures and successfully extracts the encryption code from the PIC pad. The criminal could then manufacture one new counterfeit debit card for each message that had been transmitted over that six month period. Under DUKPT, however, the criminal's theft and dissection would not allow him to decrypt previous messages (although new messages would still be decryptable if the criminal were to replace the PIC pad subsequent to dissection).

20 In the biometric-PIC situation, the criminal has an even harder time, as even if messages are decrypted, turning a digital biometric-PIC into a physical fingerprint is much harder than turning an account number-PIC into a plastic card, which is one of the significant benefits of the tokenless system.

25 Still, if a criminal can decrypt, he can encrypt, which might allow him to electronically submit a biometric-PIC to the system to

authorize a fraudulent transaction. While this is quite difficult, it is still best to restrict the options available to the criminal as much as possible, hence the use of DUKPT.

1.3. BIA Software Command Sets

1.3.1. BIA Software: Retail Command Set

The BIA/Retail software interface exports an interface that allows specific retail point of sale terminals to interact with the system.

The BIA/Retail interface is designed to allow the terminal to perform the following operation:

Transaction Authorization

In order to implement those operations, the BIA/Retail provides the following command set:

Set Language <language-name>
 Get Biometric <time>
 Get PIC <time>
 Assign Register <register> <value>
 Get Account index code <time>
 Validate Amount <amount> <time>
 Enter Amount <time>
 Form Message <type>
 Show Response <encrypted response> <time>
 Reset

1.3.2. BIA Software: CATV (Integrated Remote) Command Set

The BIA/CATV software interface exports a command set that allows terminals integrated with a Phone/CATV BIAs to interact with the system. The following operation is supported:

Remote Transaction Authorization

In order to implement that operation, the BIA/CATV provides the following command set:

5 Get Biometric <time>
 Set PIC <text>
 Assign Register <register> <text>
 Set Account index code <text>
 Form Message <type>
10 Decrypt Response <encrypted response message>
 Reset

1.3.3. BIA Software: Integrated FAX Command Set

15 The BIA/Fax software interface exports a command set that allows terminals integrated with a fax BIA to interact with the system. The following operations are supported:

20 Secure Fax Submit
 Secure Fax Data
 Secure Fax Tracking
 Secure Fax Retrieve
 Secure Fax Reject
 Secure Fax Archive
25 Secure Fax Contract Accept
 Secure Fax Contract Reject
 Electronic Document Archive Retrieve

30 In order to implement these operations, the BIA/Fax provides the following command set:

 Get Biometric <time>
 Set PIC <text>
 Set Title Index Code <text>
35 Assign Register <register> <value>
 Get Message Key

Form Message <type>
 Decrypt Response <encrypted response message>
 Reset

5 1.3.4. BIA Software: Registration Command Set

The BIA/Reg software interface exports an interface that allows
 general purpose computers to interact with the system to identify and
 register individuals. The following operations are supported:

Individual Identification
 Biometric Registration

10 In order to support those operations, the BIA/Reg provides the
 following command set:

Set Language <language-name>
 Get Biometric <time> [primary|secondary]
 Get PIC <time>
 20 Assign Register <register> <text>
 Get Message Key
 Form Message <type>
 Show Response <encrypted response> <time>
 Reset

25 1.3.5. BIA Software: PC Command Set

The BIA/PC software interface exports a command set that
 allows general purpose computers to send, receive, and sign electronic
 documents, conduct transactions across the network, and provide
 biometric-derived credentials to sites on the network. The following
 operations are supported:

35 Electronic Document Submit
 Electronic Document Data
 Electronic Document Tracking

Electronic Document Retrieve
Electronic Document Reject
Electronic Document Archive
5 Electronic Document Archive Retrieve
Electronic Signature Submission
Electronic Signature Check
Remote Transaction Authorization
Network Credential
10 Secured Connection

In order to support those operations, the BIA/PC provides the following command set:

15 Set Language <language-name>
Get Biometric <time>
Get PIC <time>
Get Account index code <time>
Validate Amount <amount> <time>
20 Enter Amount <time>
Validate Document <name> <time>
Assign Register <register> <text>
Get Message Key
Form Message <type>
25 Show Response <encrypted response> <time>
Validate Private <encrypted validation> <time>
Reset

1.3.6. BIA Software: Issuer Command Set

30 The BIA/Iss software interface exports an interface that allows general purpose computers to interact with the system to authenticate and submit batch change requests. The following operation is supported:

35 Issuer Batch

In order to implement this operation, the BIA/Iss provides the following command set:

5 Set Language <language-name>
 Get Biometric <time> [primary|secondary]
 Get PIC <time>
 Assign Register <register> <value>
 Get Message Key
 10 Form Message <type>
 Show Response <encrypted response> <time>
 Reset

1.3.7. BIA Software: Internal Command Set

15 The BIA/Int exports a command set that allows general purpose computers to interact with the system to identify individuals. The following operation is supported:

Individual Identification

20 In order to implement this operation, the BIA/Int provides the following command set:

25 Set Language <language-name>
 Get Biometric <time>
 Get PIC <time>
 Assign Register <register> <value>
 Get Message Key
 Form Message <type>
 30 Show Response <encrypted response> <time>
 Reset

1.3.8. BIA Software: ATM Command Set

35 The BIA/ATM software interface exports a command set that allows ATMs to identify individuals. The following operation is supported:

Account Access

5 In order to implement this operation, the BIA/ATM provides the following command set:

Get Biometric <time>

Set PIC <text>

Set Account index code <text>

10 Assign Register <register> <value>

Form Message <type>

Decrypt Response <encrypted response message>

Reset

15 1.4. Terminals

1.4.1. Introduction

20 The terminal is the device that controls the BIA and connects to the DPC via modem, X.25 connection, or Internet connection — methods well-known to the industry. Terminals come in different shapes and sizes, and require different versions of the BIA to perform their tasks. Any electronic device, which issues commands to and receives results from the biometric input device, can be a terminal.

25 Some terminals are application programs that run on a general purpose microcomputer, while other terminals are combinations of special purpose hardware and software.

30 While the terminal is critical for the functioning of the system as a whole, the system itself places no trust in the terminal whatsoever. Whenever a terminal provides information to the system, the system always validates it in some manner, either through presentation to the individual for confirmation, or by cross-checking through other previously registered information.

35 While terminals are able to read some parts of BIA messages in order to validate that the data was processed properly by the BIA,

terminals cannot read biometric identification information including the biometric, the PIC, encryption keys, or account index codes.

Specific BIAs export some security functionality to the terminal, such as PIC entry, and private code display. As a result, such devices are regarded as somewhat less secure than their entirely self-contained counterparts, and as such have consequently lower security ratings.

There are many different terminal types; each is connected to a specific model BIA. Each terminal is described in brief below:

ATM (Automated Teller Machinery)

Integrated BIA/ATM with ATM software load provides biometric-PIC access to ATM cash dispensers.

BRT (Biometric Registration Terminal)

Standard BIA with Registration software load attached to a microcomputer provides banks with the ability to register new individuals with the system along with their financial asset accounts and other personal information.

CET (Certified Email Terminal)

Standard BIA with PC software load attached to a microcomputer provides individuals with the ability send, receive, archive, reject, and track certified email messages.

CPT (Cable-TV Point of Sale Terminal)

BIA/catv with CATV software load attached to the CATV broadband provides individuals with biometric-television (or "TV") remotes with the ability to authorize television shopping purchases.

CST (Customer Service Terminal)

Standard BIA with Internal software load attached to a microcomputer system authorizes employees to construct database requests for the purposes of customer service.

EST (Electronic Signature Terminal)

Standard BIA with personal computer software load attached to a microcomputer provides individuals with the ability to construct and verify electronic signatures on documents.

5

IPT (Internet Point of Sale Terminal)

Standard BIA with personal computer software load attached to a microcomputer provides individuals with internet connections the ability to purchase products from a merchant that is connected to the Internet.

10

IT (Issuer Terminal)

Standard BIA with Issuer software load attached to a microcomputer provides banks with the ability to send batched changes of asset accounts to the DPC.

15

ITT (Internet Teller Terminal)

Standard BIA with personal computer software load attached to a microcomputer with an internet connection provides individuals with the ability to perform transactions with their favorite Internet Bank.

20

PPT (Phone Point of Sale Terminal)

BIA/catv with CATV software load integrated with a telephone provides individuals with the ability to authorize transactions over the telephone.

25

RPT (Retail Point of Sale Terminal)

Standard BIA with Retail software load attached to an X.25 network or using a modem allows an individual to purchase items using transaction authorizations in a store.

30

SFT (Secure Fax Terminal)

BIA/catv with Fax software load integrated with a fax machine provides individuals with the ability to send, receive, reject archive, and track secured fax messages.

35

1.4.2. Terminal: Retail Point of Sale Terminal

1.4.2.1. Purpose

5 The purpose of the RPT is to allow individuals to purchase items at a store without having to use either cash, check, or a debit or credit card.

10 The RPT uses a BIA/Retail to authorize financial transactions from an individual to a merchant. In addition to being used to accept biometric-PIC authorizations, the RPT provides standard debit and credit card scanning functions as well.

15 Note that only the biometric-related transactions are described in detail here. It is assumed that the RPT will also consist of standard credit and debit magnetic stripe card readers, as well as optional smart card readers too.

1.4.2.2. Construction

20 Each RPT is connected to the DPC by a modem, an X.25 network connection, an ISDN connection, or similar mechanism. The RPT may also be connected to other devices, such as an electronic cash register, from which it obtains the amount of the transaction and the merchant code.

25 The RPT consists of:

- an BIA/Retail
- an inexpensive microprocessor
- 9.6 kb modem/X.25 network interface hardware
- merchant identification code number in non-volatile RAM
- a DTC serial port for connecting to the BIA
- 30 • magnetic stripe card reader (known in the industry)
- ECR (electronic cash register) connection port
- optional smart card reader (known in the industry)

1.4.2.3. Identification

Two entities need to be identified for the DPC to respond positively to an BIA transaction authorization request: the individual, and the merchant.

The individual is identified by the biometric-PIC, and the merchant is identified by the DPC, which cross-checks the merchant code contained in the BIA's VAD record with the merchant code added to the transaction request by the RPT.

1.4.2.4. Operation

First, the merchant enters the value of the transaction into his electronic cash register. Then, the individual enters his biometric-PIC, his account index code, and then validates the amount. The RPT then adds the product information and the merchant code to the BIA, instructs the BIA to construct the transaction, and then sends the transaction to the DPC through its network connection (modem, X.25, etc).

When the DPC receives this message, it validates the biometric-PIC, obtains the account number using the index code, and cross-checks the merchant code in the message with the registered owner of the BIA. If everything checks out, the DPC forms and sends a credit/debit transaction to execute the exchange. The response from the credit/debit network is added to the private code to form the transaction response message, which the DPC then sends back to the RPT. The RPT examines the response to see whether or not the authorization succeeded, and then forwards the response to the BIA, which then displays the individual's private code, concluding the transaction.

1.4.2.5. Security

Messages between the RPT and the DPC are secured by encryption and MAC calculation from the BIA. The MAC allows the RPT to review the unencrypted parts of the message, but the RPT cannot change them. Encryption prevents the encrypted part of the message from being disclosed to the RPT.

Each retail BIA must be registered to a merchant. This helps to discourage BIA theft. Furthermore, because the RPT adds the merchant code onto each message, replacing a merchant's BIA with a different BIA is detected by the cross-check performed at the DPC.

1.4.3. Terminal: Internet Point of Sale Terminal

1.4.3.1. Purpose

The purpose of an Internet Point of sale Terminal (IPT) is to authorize credit and debit financial transactions from an individual at a computer to a merchant, both of whom are on the Internet.

Note that the Internet simply represents a general purpose network where a merchant, the DPC, and the IPT can all connect to each other in real time. As a result, this mechanism would work exactly the same on any other general purpose network.

1.4.3.2. Construction

The IPT consists of:

- an BIA/PC
- a microcomputer
- an Internet Shopper software application
- an Internet (or other network) connection

1.4.3.3. Identification

In addition to identifying the individual, the IPT must also identify the remote merchant who is the counterparty to the transaction. The merchant must also identify both the DPC and the IPT.

The Internet Shopper program stores the hostname (or other form of net name) of the merchant from which the purchase is taking place in order to verify the merchant's identity. Since the merchant registers all of his legitimate internet hosts with the DPC, this allows the DPC to cross-check the merchant code with the merchant code stored under that hostname to verify the merchant's identity.

1.4.3.4. Operation

First, the IPT connects to the merchant using the Internet.

5 Once a connection is established, the IPT secures it by generating and then sending a Session Key to the merchant. In order to assure that the session key is protected from disclosure, it is encrypted with the merchant's Public Key using Public Key Encryption. When the merchant receives this encrypted Session Key, he decrypts it using his Private Key. This process is called securing a connection through a Public Key Encrypted secret key exchange.

10 Once connected, the IPT downloads the merchant code, and both price and product information from the merchant. Once the individual is ready to make a purchase, he selects the merchandise he wishes to buy. Then, the individual enters the biometric-PIC using the BIA/PC, the IPT sends the merchant code, the product identification information, and the amount to the BIA, and instructs it to construct a Remote Transaction Authorization request. Then the IPT sends the request to the merchant via the secure channel.

15 The merchant is connected to the DPC via the same sort of secure connection that the IPT has with the merchant, namely, using Public Key Encryption to send a secure session key. Unlike the IPT-merchant connection, however, merchant-DPC session keys are good for an entire day, not for just one connection.

20 The merchant connects to the DPC, securing the connection using the session key, forwarding the transaction to the DPC for validation. The DPC validates the biometric-PIC, cross-checks the merchant code contained in the request with the merchant code stored under the hostname that was sent in the request, and then sends a transaction to the credit/debit network. Once the credit/debit network responds, the DPC constructs a reply message including the credit/debit authorization, an encrypted private code, and the address of the individual, and sends that message back to the merchant.

25 The merchant receives the reply, it copies the individual's mailing address out of the reply, makes note of the authorization code, and forwards the reply message to the IPT.

5 The IPT hands the reply to the BIA, which decrypts the private code and displays it on the LCD screen, indicating that the DPC recognized the individual. The IPT also shows the result of the transaction as well, be it success or failure.

1.4.3.5. Security

10 Since the system in general assumes that an adversary inhabiting the network can hijack network connections at any point, all parties must have secure communications during their realtime interactions. The main concern isn't disclosure of information, but rather insertion or redirection of messages.

15 The whole system of Public Key Encryption relies on having a trusted source for the Public Keys. These trusted sources are called Certifying Authorities, and we assume that such a source will be available on the Internet in the near future.

1.4.4. Terminal: Internet Teller Terminal

20 1.4.4.1. Purpose

25 The Internet Teller Terminal (ITT) is used to identify individuals for internet banking sessions. The DPC, the bank's computer system, and the individual are all connected to the Internet.

30 There are two main tasks. The first is providing a secure communications channel from the ITT to an internet bank. The second is providing unimpeachable identity credentials to the internet bank. Once both are accomplished, the ITT can provide a secure internet banking session. In addition, the BIA's challenge-response verification capability is used to provide additional security for all high-value and/or irregular transactions.

1.4.4.2. Construction

The ITT consists of:

- an BIA (standard PC model)
- a microcomputer
- an Internet Teller software application
- an Internet connection

The ITT accepts biometric identification using an BIA/PC connected to the microcomputer serving as the individual's Internet terminal.

1.4.4.3. Identification

Both the individual and the bank are identified by the DPC to create the network credential. The network credential includes the individual's identification as well as the context of the connection (i.e., the TCP/IP source and destination ports).

The DPC identifies the bank by cross-checking the code that the bank sends to the ITT with the bank's hostname that the ITT sends to the DPC.

1.4.4.4. Operation

First, the ITT connects to the internet bank, making sure that the bank has the computing resources required to handle a new session for the individual. If the bank has sufficient resources, it sends back the bank identification code to the ITT.

Once connected, the ITT instructs the BIA to obtain the biometric-PIC and the account index code from the individual. Then the ITT adds both the bank's hostname as well as the bank code. Using all this information, the BIA is then asked to form a network credential request message which the ITT sends to the DPC via the Internet.

When the DPC receives this message, it validates the biometric-PIC, obtains the account number using the index code, and makes sure that the bank code from the message matches the bank code stored under the

bank's hostname in the Remote Merchant database. The DPC also checks to make sure that the account number returned by the index code belongs to the bank as well. If all checks out, then the DPC creates a network credential using the individual's account identification, the time of day, and the bank code. The DPC signs this credential using Public Key Encryption and the DPC's Private Key. The DPC retrieves the bank's public key, and the individual's private code, and with the credential forms the network credential response message. The response message is encrypted using the BIA response key, and is then sent back to the ITT.

When the ITT receives the response, it hands the response message to the BIA. The BIA decrypts and then displays the individual's private code on the LCD screen. The bank's public key is stored in the Public Key register. Two random session keys are generated by the BIA. The first key, called the Shared Session Key, is revealed in plaintext to the ITT. The ITT uses this shared session key to secure the connection with the bank.

The other session key, called the Private Session Key, is not shared with the ITT. It is used for the BIA's challenge-response mechanism, a mechanism that allows the bank to obtain specific validation for non-routine transactions straight from the individual, without involving the (untrustworthy) ITT.

After receiving the Shared Session Key, the ITT asks the BIA to form a Secure Connection Request message, which includes both session keys and the network credential, and are all encrypted with the bank's public key. The ITT then sends the Secure Connection Request message to the bank.

When the bank receives the request message, it decrypts the message using its own Private Key. Then, it decrypts the actual network credential using the DPC's public key. If the network credential is valid and has not expired (a credential times out after a certain number of minutes), the individual is authorized, and the conversation continues, with the session key used to ensure security.

Whenever the individual performs any non-routine or high-value transactions, the bank may wish to ask the individual to validate those transactions for extra security. To do so, the bank sends a challenge-response message encrypted with the Private Session Key to the

ITT, which forwards that challenge-response message to the BIA. The BIA decrypts the message, displays the challenge (usually of the form "Transfer of \$2031.23 to Rick Adams OK?"), and when the individual validates by hitting the OK button, the BIA re-encrypts the response with the Private Session Key and sends that message to the ITT, which forwards it to the bank, validating the transaction.

1.4.4.5. Security

The system makes use of public key cryptography to both provide credentials and to secure communications between the ITT and the bank.

For this mechanism to function properly, the bank must know the DPC's public key, and the DPC must know the bank's public key. It is critical to the security of the system that both parties keep the respective public keys secure from unauthorized modification. Note that public keys are readable by anyone, they just cannot be modifiable by anyone. Of course, any session or secret keys must be kept secure from observation, and those secret keys must be destroyed after the session has ended.

The extra validation step for non-routine transactions is necessary because of the relative difficulty involved in securing personal computer applications on the Internet due to viruses, hackers, and individual ignorance. Banks should probably restrict routine money transfers available to ITT's to include only money transfers to well-known institutions, such as utility companies, major credit card vendors, and so on.

1.4.5. Terminal: Electronic Signature

1.4.5.1. Purpose

The electronic signature terminal (EST) is used by individuals to generate electronic signatures that cannot be forged for electronic documents. The EST either allows individuals to sign electronic documents, or verifies electronic signatures already on such documents.

1.4.5.2. Construction

The EST consists of:

- an BIA/PC
- a microcomputer
- a message digest encoder algorithm
- a modem, an X.25 connection, or an Internet connection
- an electronic signature software application

The EST uses an BIA/PC attached to a microcomputer, with events controlled by an electronic signature software application.

1.4.5.3. Identification

To create a digital signature without using some sort of public/private keyed token, three things need to be done. First, the document to be signed needs to be uniquely identified, the time of day needs to be recorded, and the individual performing the signature needs to be identified. This links the document, the individual, and the time, creating a unique time stamped electronic signature.

1.4.5.4. Operation

First the document to be signed is processed by a message digest encoding algorithm that generates a message digest code. One such algorithm is the MD5 algorithm by RSA, which is well known in the industry. By their nature, message digest algorithms are specifically designed so that it is almost impossible to come up with another document that generates the same message digest code.

Then, the individual enters his biometric-PIC using the BIA, the message digest code is handed to the BIA, the name of the document is added, and the resulting Digital Signature request message is sent to the DPC for authorization and storage.

When the DPC receives the request, it performs a biometric identity check, and once the individual is verified, it collects the message digest encoding, the individual's biometric account number, the current

5 time of day, the name of the document, and the identification of the BIA that gathered the signature, and stores them all in the Electronic Signatures Database (ESD). The DPC then constructs a signature code text string that consists of the ESD record number, the date, the time, and the name of the signer, and sends this signature code along with the individual's private code back to the EST.

10 To check an electronic signature, the document is sent through the MD5 algorithm (known in the industry), and the resulting value together with the electronic signature codes are given to the BIA along with the requesting individual's biometric-PIC, and the message is sent to the DPC. The DPC checks each signature for validity, and responds as appropriate.

15 1.4.5.5. Security

The BIA doesn't encrypt any of the data relating to electronic signatures, so document titles along with specific MD5 values are sent in plaintext. The same situation holds true for signature validations.

20 Thus while signatures cannot be forged, some of the details (including document names) are vulnerable to interception.

1.4.6. Terminal: Certified Email Terminal

25 1.4.6.1. Purpose

30 The purpose of the Certified Email Terminal (CET) is to provide individuals a way of delivering electronic messages to other individuals in the system while providing for identification of sender, verification of both receipt and recipient, and assuring confidentiality of message delivery.

35 The CET uses a BIA/PC to identify both the sender and the recipient. Security is established by encrypting the message, and then by encrypting the message key using the sender's BIA during the upload, and then decrypting the message key using the recipient's BIA during the download.

1.4.6.2. Construction

Both the transmitter and the recipient CET consists of:

- a BIA
- a microcomputer
- a modem, an X.25 connection, or an Internet connection
- the ability to receive email
- a certified electronic mail application

A CET is actually a microcomputer with an electronic mail application and a network connection which invokes the BIA to generate biometric-PIC authorizations to send and receive certified electronic mail.

1.4.6.3. Identification

In order to guarantee delivery of the message, both sender and recipients must be identified.

The sender identifies himself using his biometric-PIC when he uploads the message to the DPC. Each recipient the sender wishes to send the document to is identified either by biometric account identification number, or by fax number, and extension. In order for a recipient to download the message, he identifies himself using his biometric-PIC. This procedure resembles a person-to-person telephone call.

1.4.6.4. Operation

Message delivery starts with an individual uploading a document or message, and identifying himself using his biometric-PIC. The individual then verifies the name of the document, and the email message is encrypted and uploaded.

Once a message is uploaded, the sender receives a message identification code that can be used to request the current delivery status of the document to each of the recipients.

The DPC sends an electronic mail message to each recipient, notifying them when a certified message has arrived.

Once the recipient receives the notification, the recipient may at his leisure either choose to accept or refuse that message or a group of messages by submitting his biometric-PIC and having it validated by the DPC.

5 Once successfully transmitted to all recipients, a document is removed after a predetermined period, generally 24 hours. Individuals wishing to archive the document, along with an indication of all of the individuals to whom the message was sent may submit message archival requests prior to the deletion of the message.

10 1.4.6.5. Security

In order to effect the secure aspect of the transmission, the document is protected from disclosure en route. The CET accomplishes this using the 56-bit Message Key generated by the BIA. Since the BIA takes responsibility for encrypting the Message Key as part of the biometric-PIC, the encryption key is securely sent to the DPC.

15 When an individual downloads the message, the message key is sent encrypted along with the private code, to allow the recipient to decrypt the message. Note that it is fine to have all recipients have this message key, as they all receive the same message.

20 As with the ITT, individuals must take care to secure their CET application software from surreptitious modification, as a modified CET can send any document it wishes to once the individual validates the document name.

25 1.4.7. Terminal: Secure Fax Terminal

30 1.4.7.1. Purpose

The purpose of the secure fax terminal (SFT) is to provide individuals a way of delivering fax messages to other individuals in the system while providing for identification of sender, verification of both receipt and recipient, and assuring confidentiality of message delivery.

Each SFT uses an integrated BIA/catv to identify both the sender and the recipient. Communications security is accomplished through encryption.

1.4.7.2. Construction

Both the transmitter and the recipient SFT consists of:

- an BIA/catv
- a fax machine
- optional ISDN modem

A SFT is a fax machine connected to the DPC via a modem. The system treats faxes as just another type of certified electronic mail.

1.4.7.3. Identification

There are several different levels of security for secure faxes, but in the most secure version, the identity of the sender and all recipients is verified.

The sender identifies himself using his biometric-PIC and title index code when he sends his message to the DPC. To pick up the fax, each recipient listed identifies himself, again using biometric-PIC and title index code.

In addition, the receiving site is identified by phone number. This phone number is registered with the DPC. For secured- confidential faxes, each recipient is identified with the phone number and the extension.

1.4.7.4. Operation

There are five basic types of faxes that an SFT can send.

I. Unsecured Faxes

Unsecured faxes are equivalent to a standard fax. The sender enters the phone number of the recipient site, and sends the fax. In this case, the sender remains unidentified, and the fax is sent to a given phone

number in the hopes that it will be delivered to the proper recipient. An SFT marks the top line on all such unsecured faxes prominently as being "UNSECURED". All faxes received from non-SFT fax machines are always marked as being unsecured.

5

II. Sender-Secured Faxes

In a sender-secured fax, the sender selects the "sender-secured" mode on the fax machine, enters their biometric-PIC followed by their title index code. The fax machine then connects to the DPC, and sends the biometric-PIC information. Once the DPC verifies the individual's identity, the individual then sends the fax by feeding the document into the fax scanner. In this case, the fax is actually sent to the DPC, which stores the fax digitally. Once the entire fax arrives at the DPC, the DPC commences sending the fax to each destination, labeling each page with the name, title, and company of the sender, along with the banner of "SENDER-SECURED" at the top of each page.

10

15

III. Secured Fax

In a secured fax, the sender selects the "secured" mode on the fax machine, enters their biometric-PIC followed by their title index code, and then enters the phone numbers of the recipients. Once the system verifies the sender's identity and each of the recipients phone numbers, the individual then sends the fax by feeding the document into the fax scanner. The fax is then sent to the DPC, which stores the fax digitally. Once the entire fax arrives at the DPC, the DPC sends a small cover page to the destination indicating the pending secured fax, the sender's title and identity, as well as the number of pages waiting, along with a tracking code. This tracking code is automatically entered into the memory of the recipient's fax machine.

20

25

30

To retrieve the fax, any employee of the recipient company can select the "retrieve fax" button on his fax machine, select which pending fax to retrieve by using the tracking code, and then enter biometric-PIC. If the fax is unwanted, the individual may press the "reject fax" button, though he must still identify himself to the system in order to

35

do this. Once validated as a member of the company, the fax is then downloaded to the recipient's fax machine. Each page has "SECURED" on the top of each page, along with the sender's identity and title information.

IV. Secured Confidential Fax

In a secured-confidential fax, the sender selects the "secured-confidential" mode on the fax machine, enters his biometric-PIC followed by his title and index code, and then enters the phone number and system extension of each recipient. Once the DPC verifies the sender's identity and each of the recipients phone numbers and extensions, the individual then sends the fax by feeding the document into the fax scanner. The fax is sent to the DPC, which stores the fax digitally. Once the entire fax arrives at the DPC, the DPC sends a small cover page to each destination indicating the pending secured-confidential fax, the sender's title and identity, the recipient's title and identity, as well as the number of pages waiting, along with a tracking code. This tracking code is automatically entered into the memory of the recipient's fax. However, the only individual that can retrieve the fax is the individual whose extension code is indicated.

This individual selects the "retrieve fax" button, selects the pending fax to retrieve, and then enters his biometric-PIC. Once validated as the recipient, the fax is then downloaded to the recipient's fax machine. Each page has "SECURED-CONFIDENTIAL" on the top of each page, along with the sender's title and identity information.

V. Secured Confidential Contract Fax

This fax is processed identically to the secured-confidential fax in terms of the actual delivery of the fax to the recipients, except that the fax is titled "contract" instead of secured-confidential. In addition, the DPC automatically archives contract faxes. Any recipient may accept or reject the contract through the SFT subsequent to receiving the contract fax. Hence with the option, the DPC performs the role of an electronic notary.

5 Any fax that is sent to the system and then forwarded to the recipient may be sent to any number of recipients without tying up the sending fax machine. Additionally, the tracking number of any fax sent is entered into the memory of the fax machine; a status report on any ongoing fax can be generated at the sending machine by selecting the "status" button and then selecting the particular fax pending tracking code. The DPC issues a report that is immediately sent to the sending fax machine detailing the state of the sending for each recipient.

10 With any secured or secured-confidential fax, an option exists for either the sender or one of the recipients to archive the fax (along with the specifics as to who sent and received the fax) for future reference. To this end, any secured fax is retained for some time period (i.e., 24 hours) following successful delivery. An archival tracking code is returned to the individual whenever an archive is requested. This archival code is used to retrieve faxes and fax status reports archived with the system.

15 Archived faxes are placed on read-only secondary storage after some time period (i.e., 24 hours). Retrieving an archived fax requires human intervention, and may take up to 24 hours to perform.

20 1.4.7.5. Security

The SFT system works hard to assure the recipient of the sender's identity, and it works just as hard to assure the sender that the recipient actually acknowledged receipt of the document.

25 In order to protect against interception of the communications between the sender and recipient, the fax terminal encrypts the fax using the Message Key facility provided by the BIA. Since the BIA takes responsibility for encrypting the Message Key as part of the biometric-PIC, the encryption key is securely sent to the DPC.

30 When an individual receives a secured fax of any type, the message key is sent encrypted along with the private code, to allow the recipient to decrypt the message. Note that it is fine to have all recipients have this message key, as they all receive the same message.

1.4.7.6. Notes

Sending secured faxes is very similar to sending electronic mail, and reuses much of the same software.

It is possible to construct fax terminals that do not have integral BIA/fax devices but that have a port suitable for attaching an external BIA/pc and software appropriate for using the BIA.

1.4.8. Terminal: Biometric Registration Terminal

1.4.8.1. Purpose

The purpose of the Biometric Registration Terminal (BRT) is to register new individuals including their biometric-PIC, mailing address, private code, electronic mail addresses, a list of titles and title index codes used to send and receive electronic messages and faxes, and a list of financial asset accounts and account index codes that they can access, all using their biometric-PIC.

The objective of the enrollment process is to obtain personal information from an individual at the location of a responsible institution where that information can be validated. This includes, but is not limited to retail banking outlets, and corporate personnel departments. Each participating responsible institution has one BRT that is used by a group of employees who have been authorized to perform registrations. Each employee is accountable for each individual registered.

1.4.8.2. Construction

- an microcomputer and screen, keyboard, mouse
- an BIA/Reg
- 9.6 kb modem/X.25 network connection (known in the industry)
- a biometric registration software application

The BRT uses an attached BIA/Reg for biometric entry, and is connected to the system by a 9.6kb modem or an X.25 network connection

(known in the industry). Biometric registration terminals are located in places that are physically secure such as retail banking outlets.

1.4.8.3. Identification

5 Three entities need to be identified for the DPC to respond positively to an BIA/Reg registration request: the registering employee, the institution, and the BIA/Reg. The employee must have been authorized to register individuals for that institution.

10 The institution and the BIA are identified by cross-checking the owner of the BIA with the institution code set by the BRT. The employee identifies himself to the system by entering his biometric-PIC upon starting the registration application.

15 The institution uses its standard customer identification procedure (signature cards, employee records, personal information, etc) before registering the individual on the system. It is important for the institution to verify individual identity as assiduously as possible, since the registering individual will be empowered to transfer money from those accounts at will, and/or send electronic messages using the name of the
20 company.

1.4.8.4. Operation

25 During registration, the individual enters both a primary and secondary biometric. The individual must use both index fingers; if the individual is missing index fingers, the next inner-most finger may be used. Requiring specific fingers to be used allows the prior fraud check to work.

30 The individual is encouraged to select a primary and a secondary finger; the primary finger is given preference during the DPC identity check, so the individual should present the most-often used finger as the primary. Of course, the DPC could choose to alter the designation of primary and secondary biometrics based on operations if it turns out to be important to do so.

35 As a part of the biometric encoding process, the BIA/R determines if the individual has entered "a good print." Note that there are some individuals whose jobs result in the accidental removal of their

fingerprints, such as individuals who work with abrasives or acids. Unfortunately, these individuals cannot use the system. They are detected at this stage in the process and informed that they cannot participate.

5 The individual selects a PIC of from four to twelve digits from a series of PIC options provided by the system's central database. However, the PIC must be validated by the system. This involves two checks: one, that the number of other individuals using the same PIC aren't too great (since the PIC is used to reduce the number of individuals checked by the biometric comparison algorithm), and that the individual being registered isn't too "close", biometrically speaking, with other individuals within the same PIC group. If either happens, the enrollment is rejected, an error message is returned to the BRT, and the individual is instructed to request a different PIC. The system may optionally return with an "identical match" error condition, which indicates that the individual already has a record in the system under that PIC.

10 A PIC of 0 allows the system to assign a PIC to the individual.

The individual constructs a confidential private code consisting of a word or phrase. If the individual does not wish to construct one, a private code will be constructed randomly by the terminal.

20 The individual may also arrange their financial asset code list. This list describes which account index code points at which account (i.e. 1 for debit, 2 for credit, 3 for emergency debit, etc). Note that this can only occur if the registering institution is a bank, and only if the accounts are owned by that particular banking institution.

25 Even after registration, an individual is not actually able to perform operations using the system until a prior fraud check is completed. This generally takes a few minutes, but during times of high load, it takes up to several hours. Only if the system finds no instance of prior fraud is the individual's account activated.

30 1.4.8.5. Security

If an individual is found to have defrauded the system even once, the DPC institutes a database-wide involuntary biometric database search for the criminal. Several of these are performed each night, so individuals who are particularly wanted by the system are winnowed out of

the database by using a time consuming process during conditions of light activity.

The employees performing the registration operation identify themselves using biometric-PIC only when initially activating the registration system. This is a convenience for the employee, but a possible security problem for the system, as unattended or "temporarily borrowed" BRTs could be the source for fraud. As a result, the registration application exits after a predetermined period of no activity.

1.4.9. Terminal: Customer Service

1.4.9.1. Purpose

The purpose of the customer service terminal (CST) is to provide internal DPC support personnel access to the various aspects of the system databases. Support people need to answer inquiries by individuals, issuers, institutions, and merchants that are having trouble with the system.

1.4.9.2. Construction

The CST consists of:

- a microcomputer
- an BIA/Int
- ethernet/token ring/FDDI network interface
- a database examination and modification application

Each CST is connected to the system via a high speed local area network connection such as token ring, ethernet, fiber (FDDI), etc. Each CST has the capability to query each of the databases, and display the results of these queries. However, the CST only displays fields and records based on the privilege of the individual terminal user. For instance, a standard customer service employee won't be able to see the encryption code for a given BIA's VDB record, though they can see which merchant or individual currently owns that BIA.

1.4.9.3. Identification

5 For the CST to allow access to the database, the individual and the BIA must be identified by the system. In addition, the individual's privilege level must also be determined, so that the database can restrict access appropriately.

1.4.9.4. Operation

10 An individual using a CST starts a session by providing identification by entering their biometric-PIC. The BIA constructs an Identification Request message, and send it to the DPC for verification. Once the system verifies the individual, the CST application can operate normally, though limited by the individual's previously assigned DPC
15 privilege level.

1.4.9.5. Security

20 For security purposes, the DPC will terminate a connection to the CST application after a predetermined idle time period.

It is important that the database application cannot be modified in any manner; either deliberately, or through an unintentional introduction of a virus. To that end, individual CSTs do not have any floppy drives or other removable media. Furthermore, read access to the database
25 application executable is strictly limited to those with a need to know.

In order to protect the communications between the CST and the database from surreptitious modification or disclosure, the CST encrypts all traffic between the CST and the database. To do this, the CST generates a session key that is sent to the server during the login session
30 with the system. This session key is used to encrypt and decrypt all communications with the DPC that occur during the period.

35 Even assuming secure communications and no modified database applications, the DPC makes certain that DPC data fields that are not accessible to the individual operating the CST are not sent to the CST's database application. Likewise, at no time do any CST personnel have access to or permission to modify individual biometric information.

The DPC and the support center can be co-located, or because of the fairly tight security surrounding the CST itself, the support center can be split off on its own.

5 **1.4.10. Terminal: Issuer Terminal**

1.4.10.1. Purpose

10 The purpose of the issuer terminal is to allow employees at issuing banks to submit batch asset account modification operations to the DPC in a secure and identifiable manner.

1.4.10.2. Construction

15 The IT consists of:

- a microcomputer
- a modem, X.25 network, or Internet connection to the system
- an BIA/Iss
- a network connection to the bank's internal network

20 The Issuer Terminal uses an issuer BIA to authorize mass additions and deletions of financial asset information.

1.4.10.3. Identification

25 In this operation, the bank must be identified, a properly-authorized bank employee must be identified, and all of the individuals whose asset accounts are being added or removed must also be identified.

30 The bank is responsible for identifying the individuals who wish to add their accounts at that bank to their asset account list. As in biometric registration, this is done by the bank using signature cards and personal information. The DPC identifies the bank by cross-checking the issuer code submitted by the IT with the issuer code registered in the VAD record of the BIA/Iss. A biometric-PIC is used to identify the bank
35 employee actually submitting the batch.

1.4.10.4. Operation

5 In order to add a financial asset account, an individual gives his biometric identification number to the bank (the identification number is given to the individual during the initial biometric registration step) along with the accounts that are to be added. After the individual is properly identified, this identification code and account list are forwarded to the IT for subsequent batch submission to the system.

10 Whenever deemed appropriate by the bank, an authorized individual at the bank instructs the IT to upload the batched account additions/deletions to the DPC. To do this, the authorized individual enters his biometric-PIC, the IT adds a session key, adds the bank's issuer code, and from that the BIA/Iss constructs an Issuer Batch Request message that the IT then forwards to the DPC. The IT encrypts the batch using the message code, and then sends that as well.

15 When the system receives the Issuer Batch Request, it validates that the BIA is an BIA/Iss, that the BIA/Iss is registered to the bank claimed by the issuer code, and that the individual identified in the biometric-PIC is allowed to submit batch requests to the DPC for that bank. If so, the DPC processes all the requests, keeping track of errors as required. Once done, the DPC returns the individual's private code, along with an encrypted batch containing any errors that occurred during processing.

25 1.4.10.5. Security

30 Securing this transaction is critical for the security of the system. A criminal intent on fraud need only find a way to add other people's accounts to his biometric identification code and can then commit fraud at will. Eventually the criminal is caught, and purged from the database, but only after other people's accounts are drained by the criminal.

Encryption guarantees that the transmission between bank and DPC cannot be intercepted, and thus account numbers are protected in transit.

35 Cross-checking the bank with the BIA/Iss means that both the IT and the BIA must be compromised to submit false add/delete messages

to the DPC. Thus, the bank must ensure that the IT is physically secure, and that only authorized individuals are allowed to access it.

Requiring an individual to submit the batch provides for a responsible human to be "in the loop" whose job it is to make sure that proper bank security measures have been followed in the construction and submission of the batch.

1.4.11. Terminal: Automated Teller Machinery

1.4.11.1. Purpose

The purpose of the biometric ATM is to provide individuals access to cash and other ATM functions without having to use an Interbank card. It does this by submitting a biometric-PIC and an account index code and retrieving a bank account number. For users of the system, this replaces the Interbank card (known in the industry) + PIC mechanism as a method for identifying the account and authorizing the individual. It is assumed that all ATMs still continue to accept Interbank cards.

1.4.11.2. Construction

- a standard ATM
- an integrated BIA/ATM (scanner only)
- a connection to the DPC

The biometric ATM uses an integrated BIA/ATM to identify individuals and allow them access to financial assets using a biometric-PIC and an account index. An BIA/ATM is installed into the ATM, making use of the ATM's current PIC pad for PIC and account index code entry. The ATM is connected to the system using X.25 or modem.

The BIA/ATM is structured in such a way as to make integration with an existing ATM network as simple as possible. This results in a compromise between security and ease of integration.

1.4.11.3. Identification

5 Three entities need to be identified for the DPC to respond properly to an BIA/ATM account request: the individual, the bank, and the BIA/ATM.

10 The bank is identified by cross-checking the ATM's stored bank code with the BIA/ATM's bank code. The BIA/ATM is identified by successfully locating the BIA/ATM in the VAD, and the individual is identified through the standard biometric-PIC.

1.4.11.4. Operation

15 To access an ATM, an individual enters their biometric-PIC into the BIA along with the account index code. The BIA forms an account access request message, which is then sent to the DPC by the ATM. The DPC validates the biometric-PIC as well as the emergency account index code, and then sends the resulting asset account number along with the private code back to the ATM.

20 The ATM asks the BIA to decrypt the response, and then displays the private code on the ATM's display screen. The ATM also examines the response to see whether or not the individual is performing a standard account access, or a "duress" account access. If a duress account access is indicated, the ATM may provide false or misleading information as to the amounts available to the individual; the specifics of this behavior will vary from ATM to ATM. However, no ATM will ever provide any indication to the individual that a duress transaction is in progress.

1.4.11.5. Security

30 Messages between the ATM and the DPC are secured by encryption and MAC calculation from the BIA. The MAC means that the ATM cannot change the contents of the message without being detected, and encryption prevents the encrypted part of the message from being disclosed.

35 Because the BIA/ATM has no LCD or no PIC pad attached, it requires the ATM to provide all the text prompts and to gather all the input

from the individual. This is less secure than if the BIA were performing the operation, but as ATMs are generally physically robust, it can probably be called a wash.

5 **1.4.11.6. Notes**

10 It is between the bank and the individual to specify the behavior of an ATM when the individual indicates he is performing a transaction under duress. A particular bank may choose to limit access, or alter balance information, or a false screen may be displayed. A false screen is a display of data which has been intentionally pre-determined to be inaccurate such that a coercing party will not illegally obtain accurate data about an individual's financial assets. It is beyond the scope of the invention to specify the precise behavior of an ATM under these circumstances.

15 **1.4.12. Terminal: Phone Point of Sale Terminal**

1.4.12.1. Purpose

20 The purpose of the phone point of sale terminal (PPT) is to authorize credit or debit financial transactions from an individual using a specially-equipped telephone to make a purchase from a merchant.

25 **1.4.12.2. Construction**

 The PPT consists of:

- 30
 - an BIA/catv
 - a rapid-connect digital modem [see the VoiceView patent (known in the industry)]
 - a telephone (keypad, earpiece, microphone)
 - a microprocessor
 - a DSP (digital signal processor)
 - a standard telephone line

The PPT accepts biometric identification using an BIA/catv connected to and integrated with a cordless, cellular, or standard telephone.

1.4.12.3. Identification

In order for the DPC to authorize a transaction, both the individual and the merchant must be identified.

To identify an individual, biometric-PIC identification is used.

To identify a phone-order merchant, the merchant and all his phone numbers that individuals will call are registered with the DPC. Thus when an individual submits an authorization, he also submits the phone number he called, which is then cross-checked with the merchant's listed phone numbers.

1.4.12.4. Operation

Individuals call merchants that are selling their wares through paper catalogs, newspapers, magazines, or other basic print media mechanisms. The PPT uses a special modem that shares the telephone voice line to exchange digital information with the merchant.

Each time the individual makes a phone call, the PPT keeps track of the phone number that was typed by the user, in case the individual decides to make a purchase. A DSP is used to detect dialtone, ring, connection, and so on, in order to tell what the actual phone number entered was, as distinct from extensions, or the navigation of phone message systems, and so on.

Once a call is placed to a merchant, the salesman for the merchant digitally downloads all the relevant information to the PPT including product, price, and the merchant code. Note that when in operation, the modem disconnects the speaker.

When the product information is downloaded, the PPT then prompts the individual for the biometric-PIC, the account index code, and then asks the individual to validate the purchase amount. Then the phone number and the merchant code are added, and the message is encrypted.

The rapid-connect modem is again engaged to send the authorization information to the merchant.

When the merchant receives the authorization information, the merchant verifies that the price and product information are correct, and then forwards the transaction to the DPC using a secured communications channel using either the Internet or some other general purpose network. The connection to the DPC is secured using Public Key Encryption and a secret key exchange.

Upon receiving and decrypting a phone authorization, the DPC checks the phone number against the merchant code, validates the biometric-PIC, and then sends the transaction to the credit/debit network for authorization. If authorization succeeds, the DPC appends the buyer's address to the response message and sends the response to the merchant.

The merchant receives the response from the DPC, copies the mailing address, and forwards the message to the individual again via a brief session with the rapid-connect modem. When the transmission to the IPT is complete, a chime sounds, the modem disconnects, and the individual's private code (decrypted by the BIA) is displayed on the LCD screen. The merchant's sales rep confirms that the individual's mailing address is valid; if so, the call is terminated and the transaction is complete.

1.4.12.5. Security

One of the security concerns about phone transactions is the security of the phone system itself. Apart from the biometric identification, the central problem is making sure that the number the individual called actually reaches the merchant in question.

Note that the communications link between the PPT and the merchant isn't secured, so a purchase authorization from an individual to a merchant could be intercepted. However, no financial benefit would result from this, so it is not deemed to be important.

The security of a PPT is relatively low by necessity of price, weight, and because of the problems inherent in splitting the responsibility of PIC entry and private code decryption and presentation.

1.4.13. Terminal: Cable-TV Point of Sale

1.4.13.1. Purpose

5 The purpose of the CATV point of sale terminal (CPT) is to authorize credit or debit financial transactions from an individual in front of his television (or "TV") set to a merchant who is presenting objects for sale on television.

10 1.4.13.2. Construction

The CPT consists of:

- a BIA/catv
- a television remote control with integrated BIA/catv
- 15 • a Cable-TV digital signal decoder
- a Cable-TV remote control reader
- an on-screen display mechanism
- access to a Cable-TV broadband two-way communications channel

20 The CPT accepts biometric identification using an BIA/catv that is integrated with the television's remote control device. The remote control communicates with a television top box that itself communicates with the broadband cable television network. The terminal consists of the television remote logic that communicates with the BIA, as well as the television top box that communicates over the cable broadband network.

25 1.4.13.3. Identification

30 In this transaction, the merchant and the individual must both be identified to execute the transaction.

The individual is identified by the biometric-PIC.

35 The merchant is identified by a merchant credential, created by the CATV broadcaster at the time the product is shown on television. Each product broadcast has a merchant-product credential consisting of a merchant code, a time, a duration, and a price which is signed using Public

Key Encryption and the CATV network broadcaster's private key. This merchant-product credential can only be generated by the network broadcaster.

5 **1.4.13.4. Operation**

As a television advertisement, an infomercial, or a home shopping channel displays a product, the Cable television network also broadcasts simultaneous digital information that describes a short
10 description, price, as well as the merchant-product credential. This digital information is processed and temporarily stored by the CPT, ready to be accessed by the individual when a decision to purchase is made.

To buy something that is currently being displayed, the individual selects the on-screen display function of the special television
15 Remote, which instructs the CPT to display text information on the screen regarding the currently viewed product.

The individual is first prompted for the number of the items he wishes to buy through the on-screen display. Then he is prompted to enter his Biometric-PIC, and his account index code. Once he verifies that the
20 final purchase price is okay, the product, price, merchant code, merchant-product credential, and channel number along with the Biometric-PIC are used to construct a Remote Transaction Authorization request message. The request is sent to the merchant for authorization by way of the Cable-television broadband two-way communications channel.

25 Note that each merchant that desires to sell products in this manner must have the ability to receive order information using the broadband Cable television network.

Upon receipt of the authorization request, the merchant submits it to the DPC using a secured Internet connection or an X.25 connection.

30 If the DPC authorizes the transaction, it constructs an authorization response that includes the current mailing address of the individual in addition to the authorization code, and the encrypted private code. Once the merchant receives the authorization, he copies the authorization and the mailing address, and then forwards the authorization
35 back to the CPT, who then displays the private code to the individual, terminating the transaction.

1.4.13.5. Security

5 This architecture does not allow criminals to replay messages intercepted from the CableTV broadband, but they are able to read parts of them. If this is not desirable, then the messages may be encrypted using an optional CATV Center's public key, or other "link level" encryption between the CATV set-top box (known in the industry) and the CATV local office.

10 To secure a connection between a merchant and the DPC, the connection uses a session key changed daily that has been previously exchanged using a public key encryption key exchange system.

1.5. System Description: Data Processing Center

1.5.1. Introduction

15 The Data Processing Center (DPC) handles financial transaction authorizations and individual registration as its main responsibilities. In addition, the DPC provides storage and retrieval for secure faxes, electronic documents, and electronic signatures.

20 Each DPC site is made up of a number of computers and databases connected together over a LAN (known in the industry) as illustrated in the DPC Overview Figure (number**). Multiple identical DPC sites ensure reliable service in the face of disaster or serious hardware failure at any single DPC site. Furthermore, each DPC site has electrical power backup and multiple redundancy in all of its critical hardware and database systems.

25 DPC components fall into three categories: hardware, software, and databases. Below is a short description, by category, of each component. More detailed descriptions appear in the following sections.

1.5.1.1. Hardware

- FW Firewall Machine: the entry point of the DPC site.
- 5 GM Gateway Machine: the system coordinator and message processor.
- DPCLAN DPC Local Area Network: connects the DPC sites

1.5.1.2. Databases

- IBD Individual Biometric Database: identifies individuals from their biometric and PIC code.
- 15 PFD Prior Fraud Database: lists individuals who have defrauded the system and can check if a biometric matches any of these individuals.
- 20 VAD Valid Apparatus Database: stores information required to validate and decrypt BIA messages.
- AOD Apparatus Owner Database: stores information about the owners of BIA devices.
- 25 ID Issuer Database: identifies issuing banks that participate with the system.
- AID Authorized Individual Database: stores the list of individuals allowed to use personal or issuer BIA devices.
- 30 RMD Remote Merchant Database: stores information necessary to process transactions with telephone and cable television merchants.
- 35

EDD Electronic Document Database: stores electronic documents, such as faxes and electronic mail, for retrieval by authorized individuals.

5 ESD Electronic Signature Database: stores electronic document signatures for verification by a third party.

1.5.1.3. Software

10 MPM Message Processing Module: handles the processing of each message by coordinating with the other software modules and databases required to perform the message's task.

15 SNM Sequence Number Module: handles DUKPT sequence number processing.

MACM Message Authentication Code Module: handles MAC validation and generation.

20 MDM Message Decrypt Module: handles encrypting and decrypting of BIA requests and responses.

25 PGL PIC Group List: handles the lookup of PIC groups by PIC and the configuration of database elements that depend on the list of PIC groups.

30 IML IBD Machine List: handles the lookup of the main and backup database machines dedicated to holding IBD records for a given PIC group.

1.5.1.4. Terminology

When defining database schema, the following terminology is used for describing field types:

5

int<X>	an integral type using <X> bytes of storage
char<X>	a character array of <X> bytes
text	a variable length character array
<type>[X]	a length <X> array of the specified type.
time	a type used for storing time and date
biometric	a binary data type used for storing the biometric
fax	a binary data type used for storing fax images

10

When describing database storage requirements, the term "expected" means the expected condition of a fully loaded system.

15

1.5.2. Protocol Description

Terminals accomplish their tasks by sending request packets to a DPC site. The DPC site sends back a reply packet containing the status on the success or failure of the request.

20

Communication is via a logical or a physical connection-oriented message delivery mechanism such as X.25 connections, TCP/IP connections, or a telephone call to a modem bank. Each session holds the connection to the terminal open until the DPC sends its response back to the terminal.

25

The request packet contains a BIA message part and a terminal message part:

30

- BIA message part
 - protocol version number
 - message type
 - 4-byte BIA Identification
 - 4-byte sequence number
 - <message specific data>
 - Message Authentication Code (MAC)

35

Terminal message part
 <terminal specific data>

5 The BIA message part is constructed by an BIA device. It includes one or two biometrics, a PIC, authorization amounts, and the contents of the general registers which are set by the terminal. Note: the MAC in the BIA message part only applies to the BIA part and not to the terminal part.

10 A terminal may place additional data for the request message in the terminal message part. The BIA provides a message key to allow the terminal to secure the terminal part data. The BIA automatically includes the message key in the packet's encrypted biometric-PIC block when necessary. The terminal performs the message key encryption itself, however.

15 The response packet contains a standard header and two optional free-form message parts: one with a MAC and one without:

Standard Header

20 protocol version number
 message type

Optional Free-form message part with MAC

<message specific data>
 MAC

25 Optional Free-form message part without MAC

<additional message specific data>

30 The message part with a MAC is sent to the BIA so that it may validate that this part of the response has not been tampered with and to display the individual's private code. The message part without a MAC is used for transmitting large amounts of data, such as fax images, that are not sent to the BIA for MAC validation as the BIA to terminal connection may be of limited bandwidth.

1.5.3. Processing Packets

5 In an embodiment of the invention with multiple DPC sites, a terminal need only send its request to one of the DPC sites, typically the closest, because that site automatically handles updating the others by running distributed transactions as necessary.

10 When one of the DPC's Firewall Machines receives a packet, it forwards it to one of the GM Machines for the actual processing. Each GM has a Message Processing Module that handles the coordination between the DPC components required to process the request and sends the response back to the sender.

1.5.4. Validating and Decrypting Packets

15 All packets the DPC receives, with the exception of those not constructed by an BIA, contain an BIA hardware identification code (the BIA Identification of the packet), a sequence number, and a Message Authentication Code (MAC). The GM asks the MAC Module to validate the packet's MAC and then checks the sequence number with the Sequence
20 Number Module. If both check out, the GM passes the packet to the Message Decrypt Module for decryption. If any one of the checks fail, the GM logs a warning, terminates processing for the packet, and returns an error message to the BIA device.

25 Currently, the only message types that are not constructed by an BIA is the Secure Fax Data request and Electronic Document Data request.

1.5.5. Reply Packets

30 Each packet the DPC receives may contain an optional response key stored in the encrypted biometric-PIC block of the packet. Before the DPC replies to a request that includes a response key, it encrypts the reply packet with the response key. It also generates a Message Authentication Code and appends it to the packet.

35 The only exception to encrypting response packets applies to error messages. Errors are never encrypted and never include confidential

information. However, most response packets include a status or reply code that can indicate whether the request succeeded or not. For example, when the DPC declines a credit authorization, it does not return an error packet, it returns a normal transaction response packet with a reply code set to "failed".

1.5.6. DPC Procedures

The DPC has two procedures commonly used while processing requests.

1.5.6.1. Individual Identification Procedure

For requests that require the DPC to identify an individual, the DPC executes the following procedure: using the PIC code, the DPC searches the IBD Machine List for the main and backup IBD machines responsible for handling identifications for the given PIC code. Next, the DPC sends the identification request to either the main or backup machines depending on which is the least loaded. The IBD machine responds with the IBD record for the individual or an "individual not found" error.

The IBD machine retrieves all the IBD records for the given PIC. Using a proprietary biometric hardware device, the IBD machine compares each record's primary biometric with the individual's biometric arriving at a comparison score indicating the similarity of the two biometrics. If no biometric has a close enough comparison score, the comparisons are repeated using the secondary biometrics. If none of the secondary biometrics have a close enough comparison score, then the IBD machine returns an "individual not found" error. Otherwise, the IBD machine returns the full IBD record of the individual, from which such fields such as the private code, account numbers, titles, and so on may be obtained.

1.5.6.2. Emergency Response Procedure

For requests that include an account index, the DPC handles the case where the individual chooses his or her emergency account index. The

GM processing the request immediately notifies the DPC customer support staff, logs a warning, and if the response packet has a reply code, sets it to "emergency". It is the responsibility of the owner of the BIA device that submitted the request to watch for an "emergency" reply code and provide further assistance, such as the false screen mechanism described in the ATM terminal section. The DPC also increments the emergency use count of the individual's IBD record whenever the emergency account index gets accessed.

1.5.7. Protocol Requests

The following sections describe each protocol request/response and the actions the DPC takes to perform them.

The list of protocol packets are:

- Individual Identification
- Transaction Authorization
- Registration
- Account Access
- Issuer Batch
- Secure Fax Submit
- Secure Fax Data
- Secure Fax Tracking
- Secure Fax Retrieve
- Secure Fax Reject
- Secure Fax Archive
- Secure Fax Contract Accept
- Secure Fax Contract Reject
- Secure Fax Organization Change
- Electronic Document Submit
- Electronic Document Data
- Electronic Document Tracking
- Electronic Document Retrieve
- Electronic Document Reject
- Electronic Document Archive

- Electronic Document Archive Retrieve
- Electronic Signature
- Electronic Signature Verify
- Network Credential

5

1.5.7.1. Individual Identification

Individual Identification Request

BIA Part:

10

4-byte BIA Identification

4-byte sequence number

encrypted(DUKPT key) Biometric-PIC block:

300-byte authorization biometric

4-12 digit PIC

15

56-bit response key

MAC

Terminal Part: (not used)

Individual Identification Response

20

encrypted(response key):

private code text

individual name

biometric identification code

MAC

25

The Individual Identification request includes a biometric-PIC block which the DPC uses with the individual identification procedure to identify the individual. If the individual is identified, then the DPC responds with the individual's name, biometric identification, and private code. Otherwise, the DPC responds with an "unknown individual" error.

30

1.5.7.2. Transaction Authorization

Transaction Authorization Request

BIA Part:

- 5 4-byte BIA Identification
- 4-byte sequence number
- encrypted(DUKPT key) Biometric-PIC block:*
- 300-byte authorization biometric
- 4-12 digit PIC
- 10 56-bit response key
- [optional 56-bit message key]
- account index
- price
- merchant Identification
- 15 [optional free-format product information]
- [optional merchant code (phone#, channel# + time, hostname)]
- [optional send-address request]
- MAC

Terminal Part: (not used)

20

Transaction Authorization Response

encrypted(response key):

- private code text
- authorization response
- 25 authorization detail (autho code, transaction identification, etc)
- [optional individual address information]
- reply code (fail, ok, emergency)
- MAC

30

There are two basic transaction authorization subtypes: retail and remote.

For retail authorizations, the DPC identifies the purchasing individual by the biometric-PIC block of the request. If the individual cannot be identified, the DPC replies with an "unknown individual" error.

35

Next, the DPC sends an external authorization request (crediting the asset account of the BIA device's owner and debiting the

individual's asset account) to one of several existing financial authorization services depending on the type of asset accounts involved (such as Visa™ or American Express™). If the external financial authorization service approves the transaction, the DPC returns the external authorization codes and an "ok" reply code to the BIA device. Otherwise, the DPC returns the reason why the authorization was denied and sets the reply code to "failed". In either case, the DPC includes the individual's private code in the response.

When the DPC looks up the individual's asset account using the account index of the request, the chosen account may be the "emergency" account. If this happens, the DPC follows the emergency response procedure. The external authorization still takes place, however.

Remote authorization are generated by telephone, mail- order, or cable television merchants. The DPC handles remote authorizations the same way it does a retail authorization but with the following exceptions:

i) Remote authorizations include a remote merchant code which the DPC checks against the Remote Merchant Database to validate whether the packet's merchant Identification matches the one stored in the database. Furthermore, the asset account credited is the remote merchant's account, not the account of the BIA device's owner.

ii) Additionally, BIA devices that generate the remote authorizations tend to be personal BIA devices. The DPC checks the biometric Identification of the identified individual against the Authorized Individual Database's list of individuals allowed to use the BIA device. If the individual is not authorized to use the device, then the DPC denies the authorization request.

iii) Finally, the authorization packet may contain a "send-address" indicator. This indicator informs the DPC to include the individual's address in the reply packet and is usually used only for mail order purchases.

1.5.7.3. Registration

Registration Request

BIA Part:

- 4-byte BIA Identification
- 4-byte sequence number

encrypted(DUKPT key) Biometric-PIC block:

1000-byte primary biometric

1000-byte secondary biometric

4-12 digit PIC

5 56-bit response key

56-bit message key

MAC

*Terminal Part:**encrypted(message key):*

10 name

address

zipcode

private code

15 asset account list (account index code, account #)

emergency account (account index code, account #)

title list (title index code, title name)

Registration Response

status code

20 *encrypted(response key):*

private code text

PIC

biometric Identification code

25 list of DPC chosen PICs (if original choice of PIC
is rejected)

status code (ok, rejected)

MAC

30 Individuals register with the DPC via a Biometric Registration Terminal (BRT). The BRT sends the DPC a registration packet containing primary and secondary biometrics and personal identification code, along with ancillary data such as the individual's name, address, a list of financial asset accounts, the private code, and the emergency account. Optionally, the individual may include an electronic mail address, and a title list

35 including titles and the title index code, as well as an Social Security Number (or "SSN"). The individual may choose his or her own PIC code

or allow the system to choose it. In a modification step any previously entered data can be modified or deleted.

At any given moment, only one DPC site acts as the registration site, for implementation simplicity. Registration request packets received by non-registration DPC sites are forwarded to the current registration site. The registration DPC site performs the entire registration check, assigning of IBD records to IBD machines, and the distributed transaction required to update all other DPC sites.

The registration DPC site selects the PIC code for registration requests that don't specify one, stores the IBD record on the main and backup IBD machines (as specified in the PIC Group List), and checks the PIC and biometric suitability of the registration packet before running the distributed transaction to update the other DPC sites.

The DPC runs a personal identification code and biometric sample duplication check step wherein the biometrics and personal identification code gathered during the registration step is checked against all previously registered biometrics currently associated with the identical personal identification code. The DPC may reject the registration for the following reasons: the PIC code is too popular, or the biometrics are too similar to other biometrics stored under the chosen PIC. To aid the individual in choosing an acceptable PIC, the DPC generates a short list of PIC codes for which the registration will be guaranteed that it reserves for a period of time. The BRT then prompts the individual for a new PIC which may be chosen from the good PIC list.

1.5.7.4. Account Access

Account Access Request

BIA Part:

4-byte BIA Identification

4-byte sequence number

encrypted(DUKPT key) Biometric-PIC block:

300-byte authorization biometric

4-12 digit PIC

56-bit response key

[optional 56-bit message key]

account index

MAC

Terminal Part: (not used)

5

Account Access Response

encrypted(response key):

private code text

[optional PIC]

asset account number

10

reply code (fail, ok, emergency)

MAC

The account access request allows BIA-equipped Automated Teller Machines to provide a safer and more convenient way for individuals to identify themselves to the ATM.

15

The GM identifies the individual by the packet's biometric-PIC and uses the specified account index to choose which asset account number to retrieve.

When the GM looks up the individual's asset account using the account index of the request, the chosen account may be the "emergency" account. If this happens, the GM follows the emergency response procedure.

20

1.5.7.5. Issuer Batch

25

Issuer Batch Request

BIA Part:

4-byte BIA Identification

4-byte sequence number

30

encrypted(DUKPT key) Biometric-PIC block:

300-byte authorization biometric

4-12 digit PIC

56-bit response key

56-bit message key

35

issuer code

MAC

*Terminal Part:**encrypted(message key) batch list:*

add <biometric Id> <account index> <asset account> [<emergency flag>]
 remove <biometric Id> <account index> <asset account>

Issuer Batch Response*encrypted(response key):*

private code text
 reply code (fail, ok, emergency)
 MAC

encrypted(message key) failed list:

failed <command> <code>

...

The Issuer Batch request allows an issuing bank or other authority to perform routine maintenance on the Individual Biometric Database. The DPC logs a security violation warning if it receives any Issuer Batch requests from non-issuer BIA devices, and it also refuses to process the request.

The DPC identifies the individual submitting the batch request by following the individual identification procedure. The DPC then checks that the individual is registered in the Authorized Individual Database to use the BIA device embedded in the sending Issuer Terminal.

The DPC also uses the issuer code in the request to look up the apparatus owner Identification in the Issuer Database and compare it against the apparatus owner Identification stored in the Valid Apparatus Database to ensure that the issuer code is not forged.

The DPC then executes the add and delete commands in the message-key encrypted batch list. The batch list is a newline separated list of commands. Valid commands are:

add <biometric Id> <account index> <asset account> [<emergency flag>]
 remove <biometric Id> <account index> <asset account>

The add command adds the asset account to the account list at the specified account index. The optional emergency flag indicates whether the particular account index is treated as the individual's emergency account. If the

asset account currently stored in the account list does not belong to the issuer, the command fails. This feature prevents one bank from adding or removing asset accounts from other bank's customers without the individual's knowledge or authorization.

5 The remove command clears the individual's asset account stored at the specified account index in the account list. If the asset account currently stored in the account list does not match the account the issuer is attempting to remove, the command fails.

10 For each command in the batch that failed to execute correctly, the GM logs a security violation warning and appends an entry to the failed list of the response. The failed entry includes the text for the command and the error code.

15 **1.5.7.6. Secure Fax Submit**

Secure Fax Submit Request

BIA Part:

 4-byte BIA Identification

 4-byte sequence number

20 *encrypted(DUKPT key) Biometric-PIC block:*

 300-byte authorization biometric

 4-12 digit PIC

 56-bit response key

 56-bit message key

25 security mode (unsecured, sender-secured, secured, secured-confidential)

 sender title index code

 sender fax number

 sender fax extension

 recipient list

30 [optional archive fax indicator]

 [optional contract/agreement indicator]

Terminal Part: (not used)

Secure Fax Submit Response

encrypted(response key):

private code text

fax tracking number

MAC

5

When the DPC receives a Secure Fax Submit request, it identifies the individual from the request's biometric-PIC by following the individual identification procedure. This identification, along with the individual's title described by the title index code, is presented to the recipients so that the sender of the fax is always reliably identified.

10

The DPC generates a tracking number for tracking purposes and stores it, the sender's biometric Identification, the security mode, and the message key in a newly created EDD Document record. For each recipient in the recipient list, the DPC also creates a Recipient record. The DPC then waits for the sending fax machine to transmit the fax data encrypted under the message key.

15

If the request includes an "archive fax" or "contract/agreement" indicator, the EDD places a copy of the Document and Recipient records in the archive database. Any subsequent updates to these records are also made to the archived versions.

20

The fax data is sent in a separate step so that if the sender makes a mistake entering his biometric and PIC, the system notifies him before he wastes any time feeding the document into the fax machine.

25

1.5.7.7. Secure Fax Data

Secure Fax Data Request

BIA Part: (not used)

Terminal Part:

fax tracking number

encrypted(message key):

fax image data

30

Secure Fax Data Response

status (incomplete, ok)

35

The Secure Fax Data request allows a secure fax machine to send the fax image to the DPC for delivery to the previously specified recipient(s). This request does not involve any biometric identification and instead relies upon the secret message key to securely transmit the image.

5 The fax image data is encrypted by the message key registered by the Secure Fax Submit request. Once the DPC has received the entire fax, it sends a Secure Fax Arrival Notice message to each of the recipient's fax numbers. The DPC retrieves the list of recipients by querying the EDD for all
10 Recipient records containing the fax tracking number. The Recipient record contains the destination fax number and optional extension. After sending the Arrival Notice, the DPC updates each Recipient record's delivery status field to "notified". Note: if the destination fax number is busy, the DPC marks the
15 delivery status field to "busy" and retries sending the notice periodically (i.e., every 10 minutes) until successful and at that time, updates the status field to "notified".

The Arrival Notice is as follows:

Secure Fax Arrival Notice (Fax message)

20 sender name, company, title, and fax number
 fax tracking number
 instructions on how to download the fax

25 The DPC only sends the sender a Status Notice via fax after all recipients have either retrieved or rejected the fax. The sender may query the DPC using the Secure Fax Tracking request (see below) to get the current status of all recipients.

The Status Notice is as follows:

Secure Fax Status Notice (Fax message)

30 sender name, company, title, and fax number
 fax tracking number
 list of recipients showing:
 name, company, title, and fax number
 delivery date and status
35 contract/agreement status

The DPC finds each individual's company and title information in the EDD Organization table.

For individuals who are not registered in the system and hence cannot receive secure faxes or for non-recipient secured modes, the DPC does not send them a Secure Fax Arrival Notice. Instead, the DPC sends them the fax directly. If the fax line is busy, the DPC retries every 10 minutes until it succeeds in delivering the fax.

1.5.7.8. Secure Fax Tracking

Secure Fax Tracking Request

BIA Part:

4-byte BIA Identification

4-byte sequence number

encrypted(DUKPT key) Biometric-PIC block:

300-byte authorization biometric

4-12 digit PIC

56-bit response key

56-bit message key

fax tracking number

MAC

Terminal Part: (not used)

Secure Fax Tracking Response

encrypted(response key):

private code text

message digest for tracking response fax image

status code (ok, failed)

MAC

fax image for recipient status list

The DPC handles the Secure Fax Tracking request by retrieving all EDD Recipient records for the fax and generating a fax message to display the records. If the individual making the tracking request is not the sender of the fax document, then the DPC sets the status code to failed and puts an empty fax in the response.

The tracking response fax contains information describing the status of the delivery of the fax to each recipient. This fax contains such status information as line busy, fax arrival notice sent, fax sent, fax rejected, contract accepted, and so on.

5

The Tracking Notice is as follows:

Secure Fax Tracking Notice (Fax message)

sender name, company, title, and fax number

fax tracking number

10

list of recipients showing:

name, company, title, and fax number

delivery date and status

contract status

15

1.5.7.9. Secure Fax Retrieve

Secure Fax Retrieve Request

BIA Part:

4-byte BIA Identification

20

4-byte sequence number

encrypted(DUKPT key) Biometric-PIC block:

300-byte authorization biometric

4-12 digit PIC

56-bit response key

25

fax tracking number

MAC

Terminal Part: (not used)

Secure Fax Retrieve Response

30

encrypted(response key):

private code

56-bit message key

status (incomplete, ok, invalid recipient)

message digest for fax image

35

MAC

encrypted(message key):

fax image

5 The DPC uses the biometric-PIC to identify the individual making the retrieve request by following the individual identification procedure. If no EDD Recipient record exists for the individual and for the specified fax, then the DPC responds with an "invalid recipient" status.

The DPC retrieves the encrypted fax image from the EDD Document record with the correct fax tracking number and biometric Identification which it returns to the requester.

10 The fax image includes a cover page that displays whether the fax is a contract/agreement and the sender's name, company, title, fax number, and extension.

15 When the last recipient has either received or rejected the fax, the DPC sends a Status Notice via fax (see Secure Fax Data, above) to the fax's sender and then schedules to remove the Document and Recipient records from the EDD within a configurable time period. The time period is intended to allow the recipients sufficient time to decide whether or not to archive the fax.

20 1.5.7.10. Secure Fax Reject

Secure Fax Reject Request

BIA Part:

25 4-byte BIA Identification

4-byte sequence number

encrypted(DUKPT key) Biometric-PIC block:

300-byte authorization biometric

4-12 digit PIC

56-bit response key

30 fax tracking number

MAC

Terminal Part: (not used)

Secure Fax Reject Response

encrypted(response key):

35 private code

status code (ok, invalid recipient)
 MAC

5

The DPC uses the biometric-PIC to identify the individual making the secure fax reject request. The DPC finds the EDD Recipient record keyed by the request's fax tracking number and the individual's biometric Identification. If the record cannot be found then the request fails with an "invalid recipient" status.

10

When the last recipient has either received or rejected the fax, the DPC sends a Status Notice via fax (see Secure Fax Data, above) to the fax's sender and then schedules to remove the Fax and Tracking records from the EDD within a configurable time period. The time period is intended to allow the recipients sufficient time to decide whether or not to archive the fax.

15

1.5.7.11. Secure Fax Archive

Secure Fax Archive Request

BIA Part:

20

4-byte BIA Identification
 4-byte sequence number
encrypted(DUKPT key) Biometric-PIC block:
 300-byte authorization biometric
 4-12 digit PIC
 56-bit response key
 fax tracking number
 MAC

25

Terminal Part: (not used)

Secure Fax Archive Response

30

encrypted(response key):
 private code
 status code (ok, invalid individual)
 MAC

35

The DPC uses the biometric-PIC to identify the individual making the secure fax archive request. The DPC finds the EDD Recipient record keyed

by the request's fax tracking number and the individual's biometric Identification. If the record cannot be found and the individual is not the sender or one of the recipients, then the request fails with an "invalid individual" status. Otherwise, the DPC copies the Document and Recipient records into the EDD archive database. Any subsequent changes to these records are also copied to the archived versions.

1.5.7.12. Secure Fax Contract Accept

Secure Fax Contract Accept Request

BIA Part:

4-byte BIA Identification

4-byte sequence number

encrypted(DUKPT key) Biometric-PIC block:

300-byte authorization biometric

4-12 digit PIC

56-bit response key

fax tracking number

MAC

Terminal Part: (not used)

Secure Fax Contract Accept Response

encrypted(response key):

private code

status code (ok, invalid recipient)

MAC

The DPC uses the biometric-PIC to identify the individual making the Contract Accept request. The DPC finds the EDD Recipient record keyed by the request's fax tracking number and the individual's biometric Identification. If the record cannot be found then the request fails with an "invalid recipient" status. Otherwise, the DPC updates the Recipient record's contract status field to "accepted" and generates a Status Notice to the fax's sender (see Fax Data, above).

1.5.7.13. Secure Fax Contract Reject

Secure Fax Contract Reject Request

BIA Part:

- 5 4-byte BIA Identification
- 4-byte sequence number
- encrypted(DUKPT key) Biometric-PIC block:*
- 300-byte authorization biometric
- 4-12 digit PIC
- 10 56-bit response key
- fax tracking number
- MAC

Terminal Part: (not used)

Secure Fax Contract Reject Response

- 15 *encrypted(response key):*
- private code
- status code (ok, invalid individual)
- MAC
- 20

25 The DPC uses the biometric-PIC to identify the individual making the Contract Reject request. The DPC finds the EDD Recipient record keyed by the request's fax tracking number and the individual's biometric Identification. If the record cannot be found then the request fails with an "invalid recipient" status. Otherwise, the DPC updates the Recipient record's contract status field to "rejected" and generates a Status Notice to the fax's sender (see Fax Data, above).

1.5.7.14. Secure Fax Organization Change

- 30 Secure Fax Organization Change (Secure Fax message)
- sender name, company, title, and fax number
- list of organizational changes

35 Organization changes are submitted to the DPC via a secure fax message. A customer support engineer enters the changes requested in the fax

message, verifying that the individual submitting the request is allowed to register individuals for that particular company. Since the fax is a secure fax, the sender's identity has already been ascertained, as has his title.

5 **1.5.7.15. Electronic Document Submit**

Electronic Document Submit Request

BIA Part:

4-byte BIA Identification

4-byte sequence number

encrypted(DUKPT key) Biometric-PIC block:

300-byte authorization biometric

4-12 digit PIC

56-bit response key

56-bit message key

recipient list

MAC

Terminal Part: (not used)

20 **Electronic Document Submit Response**

encrypted(response key):

private code text

tracking number

status code (ok, invalid recipient)

25 MAC

When the DPC receives an Electronic Document Submit request, it identifies the individual by following the individual identification procedure.

30 The DPC then creates an EDD Document record and assigns it a unique tracking number. The DPC initializes the record's sender identification code to be the biometric identification code of the identified individual and the message key to be the message key in the request.

35 Next, the DPC searches the Individual Biometric Database for each recipient and creates an EDD Recipient record for each one. Each record is initialized with the tracking number, the recipient's biometric identification

code, and a delivery status of "incomplete". If any of the recipients cannot be found, the DPC replies with an "invalid recipient" status.

1.5.7.16. Electronic Document Data

5

Electronic Document Data Request

BIA Part: (not used)

Terminal Part:

tracking number
 command (either abort or data)
 [optional message offset]
 completion indication
encrypted(message key):
 message body

10

15

Electronic Document Data Response

status (incomplete, ok)

The Electronic Document Data request allows an individual to send the document text (in one or more parts) to the EDD for delivery to the recipient(s). This request does not involve any biometric identification, instead, it relies upon the secret message key to securely transmit the document text.

20

The request text is assumed to be encrypted by the message key stored in the EDD document record and is appended to the document text already stored in the record.

25

When the EDD receives a packet with the "document complete" indicator, it knows that the sender has finished transmitting the document. The EDD now sends an Arrival Notice to all recipients of the document via Internet electronic mail informing them that they have a document waiting.

30

The Arrival Notice is as follows:

Electronic Document Arrival Notice (Internet E-mail message)

sender name, company, title, and e-mail address

tracking number

instructions on how to receive the electronic document

35

The EDD also updates the status of the EDD recipient record to "notified". When all recipients have either retrieved or rejected the electronic document, the DPC sends a Status Notice via Internet electronic mail to the document originator.

5

The Status Notice is as follows:

Electronic Document Status Notice (Internet E-mail message)

sender name, company, title, and e-mail address

tracking number

10

list of recipients showing for each

name, company, title, e-mail address

delivery date and status

15

The DPC finds each individual's company and title information in the EDD Organization table.

1.5.7.17. Electronic Document Retrieve

Electronic Document Retrieve Request

20

BIA Part:

4-byte BIA Identification

4-byte sequence number

encrypted(DUKPT key) Biometric-PIC block:

25

300-byte authorization biometric

4-12 digit PIC

56-bit response key

tracking number

MAC

30

Terminal Part: (not used)

Electronic Document Retrieve Response

encrypted(response key):

private code

56-bit message key

status (incomplete, ok, invalid recipient)

MAC

encrypted(message key):

document text

The DPC uses the biometric-PIC to identify the individual making the electronic document retrieve request by following the individual identification procedure.

The DPC next finds the EDD Recipient record keyed by the tracking number and the individual's biometric Identification.

If the record cannot be found, then the request fails with an "invalid recipient" status. Otherwise, the DPC sends the document's message key and the document (still encrypted by the message key) to the requester.

The EDD then updates the status of the EDD recipient record to "retrieved". When all recipients have either retrieved or rejected the document, the DPC sends a Status Notice via Internet electronic mail to the document originator (see Electronic Document Data, above) and then schedules to remove the Document and Recipient records (see Secure Fax Retrieve, above).

1.5.7.18. Electronic Document Reject

Electronic Document Reject Request

BIA Part:

4-byte BIA Identification

4-byte sequence number

encrypted(DUKPT key) Biometric-PIC block:

300-byte authorization biometric

4-12 digit PIC

56-bit response key

message tracking number

MAC

Terminal Part: (not used)

Electronic Document Reject Response*encrypted(response key):*

private code

status code (ok, invalid recipient)

MAC

The DPC uses the biometric-PIC to identify the individual making the electronic document reject request. The DPC next finds the EDD Recipient record keyed by the tracking number and the individual's biometric Identification. If the record cannot be found, then the request fails with an "invalid recipient" status.

The EDD updates the status of the EDD recipient record to "rejected". The DPC then follows the same notification and deletion procedure as described in Electronic Document Retrieve, above.

1.5.7.19. Electronic Document Archive**Electronic Document Archive Request***BIA Part:*

4-byte BIA Identification

4-byte sequence number

encrypted(DUKPT key) Biometric-PIC block:

300-byte authorization biometric

4-12 digit PIC

56-bit response key

tracking number

MAC

*Terminal Part: (not used)***Electronic Document Archive Response***encrypted(response key):*

private code

status code (ok, invalid individual)

MAC

The DPC uses the biometric-PIC to identify the individual making the electronic document archive request. The DPC finds the EDD Recipient record keyed by the request's tracking number and the individual's biometric Identification. If the record cannot be found and the individual is not the sender or one of the recipients, then the request fails with an "invalid individual" status. Otherwise, the DPC copies the Document and Recipient records into the EDD archive database. Any subsequent changes to these records are also copied to the archived versions.

1.5.7.20. Electronic Document Archive Retrieve

Electronic Document Archive Retrieve Request

BIA Part:

4-byte BIA Identification

4-byte sequence number

encrypted(DUKPT key) Biometric-PIC block:

300-byte authorization biometric

4-12 digit PIC

56-bit response key

optional title index code, sending fax number, and extension tracking number

MAC

Terminal Part: (not used)

Electronic Document Archive Retrieve Response

encrypted(response key):

private code

status code (ok, invalid individual)

MAC

The DPC can receive an Electronic Document Archive Retrieve request from either a Secure Fax Terminal or a Certified Email Terminal. The DPC uses the individual identification procedure to determine the individual submitting the archive retrieve request. The individual must be either the sender or one of the recipients or else the DPC denies the request by setting the status code to "invalid individual". However, if the archived document was

a fax sent using a corporate title, the DPC allows additional individuals whose titles are higher in the corporate hierarchy to retrieve the archived document as well.

5 The EDD maintains an archive database, indexed by the document's original tracking number, stored on off-line media such as CD-ROMs and tape that can take considerable time to search for the archived document. As a result, the DPC does not return the archived document immediately, but instead informs the requesting individual that the DPC has begun the search. At 10 a later date when the DPC finishes the search, it notifies the requester that the archived document is ready to be retrieved through the standard document arrival notification mechanisms -- either via fax or email, depending on the format of the original document.

15 The DPC creates an EDD archive request record to store information about the requester so that when the search completes, the DPC remembers to whom to send the document.

1.5.7.21. Electronic Signature

Electronic Signature Request

BIA Part:

4-byte BIA Identification

4-byte sequence number

encrypted(DUKPT key) Biometric-PIC block:

300-byte authorization biometric

4-12 digit PIC

56-bit response key

document name

document MD5 calculation

MAC

Terminal Part: (not used)

Electronic Signature Response

encrypted(response key):

private code text

signature string

MAC

To process the electronic signature request, the DPC first performs a biometric identification using the biometric-PIC. Then, the DPC creates an ESD record, assigns it a unique signature identification code, and sets the record's signature field to the electronic signature in the request. The DPC then returns a signature string that can be submitted for later verification:

"<Dr. Bunsen Honeydew> <Explosions in the Laboratory> 5/17/95 13:00
PST 950517000102"

1.5.7.22. Electronic Signature Verify

Electronic Signature Verification Request

BIA Part:

4-byte BIA Identification

4-byte sequence number

encrypted(DUKPT key) Biometric-PIC block:

300-byte authorization biometric

4-12 digit PIC

56-bit response key

signature string

MAC

Terminal Part: (not used)

Electronic Signature Verification Response

encrypted(response key):

private code text

signature string

status (verified, failed)

MAC

The DPC performs a biometric identification, extracts the signature tracking code from the signature string, retrieves the indicated ESD record, and verifies that it matches the signature string. The DPC returns the private code and the outcome of the signature comparison.

1.5.7.23 Network Credential

Network Credential Request

BIA Part:

5 4-byte BIA Identification
 4-byte sequence number
 encrypted(DUKPT key) Biometric-PIC block:
 300-byte authorization biometric
 4-12 digit PIC
 10 56-bit response key
 account index
 bank code
 bank hostname
 terminal.port and bank.port (TCP/IP addresses)
 15 MAC

Network Credential Response

encrypted(response key):

 private code
 20 *signed(DPC's private key):*
 credential(time, acct, terminal.port, bank.port)
 bank's public key
 status code (ok, failed)
 25 MAC

 The DPC identifies the individual using the request's biometric-PIC and retrieves the individual's asset account stored at the specified index. If the account index is the emergency account, then the network credential response status code is set to "failed" and no credential is generated.

30 The DPC constructs the credential using the current time, the retrieved asset account, and the TCP/IP addresses of the terminal and the bank. The DPC then uses public key encryption to sign the credential with its private key.

35 The response also includes the bank's public key, which the DPC retrieves from the Remote Merchant Database.

1.5.8. Customer Support and System Administration Messages

5 The DPC handles additional message types classified as internal messages. The DPC generally does not accept these messages from non-DPC systems. The messages are database vendor specific. However, the internal network uses DES-encrypted packets to provide additional security.

The Customer Service and System Administration tasks are implemented using the database vendor's query language and application development tools.

1.5.8.1. Customer Service tasks:

- IBD: find, activate, deactivate, remove, correct records.
- AID: add or remove authorized individuals.
- 15 • AOD: find, add, remove, correct records.
- VAD: find, activate, deactivate, remove, correct records.
- RMD: find, add, remove, correct records.
- PFD: add, remove, correct records.

1.5.8.2. System Administration tasks:

- Run prior fraud checks.
- Modify the Valid Site List.
- Summarize log information (warnings, errors, etc.).
- 25 • Modify the PIC Group List.
- Performance monitoring.
- Run backups.
- Crash recovery procedures.
- Time synchronization for the DPC sites.
- 30 • Change the primary registration site.
- Change the secret DES encryption key.
- Clean up old document tracking numbers.
- Generate a list of BIA hardware identification code, MAC encryption key, and DUKPT Base Key triples. Store on an encrypted floppy
35 for the Key Loading Device.

1.5.9. Firewall Machine

1.5.9.1. Purpose

5 The FW Machines provide a first line of defense against network viruses and computer hackers. All communication links into or out of the DPC site first pass through a secure FW Machine.

1.5.9.2. Usage

10 The FW Machine, an internet-localnet router, only handles messages destined for the GM Machines.

15 BIA-equipped terminals send packets to a single DPC site via modem, X.25, or other communication medium. The DPC relies on a third party to supply the modem banks required to handle the volume of calls and feed the data onto the DPC backbone.

20 For DPC to DPC communication, primarily for distributed transactions and sequence number updates, the FW Machines send out double-length DES encrypted packets. The DPC LAN component handles the encryption and decryption: the FWs do not have the ability to decrypt the packets.

1.5.9.3. Security

25 A properly configured network sniffer acts as an intruder detector as backup for the FW. If an anomalous message is detected, the intruding messages are recorded in their entirety, an operator is alerted, and the FW is physically shut down by the sniffer.

30 The FW disallows any transmissions from the internal network to the rest of the Internet.

1.5.9.4. Message Bandwidth

35 A transaction authorization request requires about 400 bytes and registration packets require about 2 KB. To handle 1000 transaction authorizations per second and 1 registration packet per second, the FW

Machines are able to process about 400 KB per second (all known in the industry) .

Each DPC site requires an aggregate bandwidth of nearly three T1 connections to the third party modem bank and the other DPC sites.

1.5.10. Gateway Machine

1.5.10.1. Purpose

The GM Machine (GM), through the FW Machines, link the outside world (BIA-equipped terminals and other DPCs) to the internal components of the DPC. The DPC has multiple GMs, typically two.

1.5.10.2. Usage

The GM supervises the processing of each BIA request, communicates with the various DPC components as necessary, and sends the encrypted results of the request back to the sender. The software performing this task is called the Message Processing Module.

The GM logs all requests it receives and any warnings from components it communicates with. For example, the GM logs any emergency account accesses, sequence number gaps, and invalid packets.

Processing a request may require the GM to inform GMs at all other DPCs of a change in the DPC databases. When this happens, the GM runs a distributed transaction to update the remote databases.

Distributed transactions fall into two categories: synchronous and asynchronous. Synchronous distributed transactions require the GM to wait for the distributed transaction to commit before continuing to process the packet. Asynchronous distributed transactions do not require the GM to wait for the commit, and allow it to finish processing the request regardless of whether the distributed transaction commits or not. Asynchronous distributed transactions are only used to update data for which database consistency is not an absolute requirement: sequence numbers and biometric checksum recordings may be performed asynchronously, whereas creating database records, such as Individual Biometric records, may not.

When executing a synchronous distributed transaction, the requesting GM only considers the entire transaction successful if all sites can successfully commit the transaction locally. Otherwise, the GMs back out the changes locally and reject the request due to a transaction error.

5 The list of valid DPC sites is normally all of the sites. In the case of an extreme site failure, however, a system administrator may manually remove that site from the valid site list. The most likely cause of distributed transaction failures, however, are temporary network failures that are unrelated to any DPC equipment. Requests that require a synchronous distributed transaction cannot be performed until network connectivity is restored or the site is removed from the valid site list. Before a site can be added back to the valid site list, the system administrator brings the site's databases up to date with those of a currently active site.

15 **1.5.10.3. Software Components**

Each GM runs the following software components locally for performance reasons:

20 **Message Processing Module**
Message Authentication Code Module
Message Decrypt Module
Individual Biometric Database Machine List

25 **1.5.10.4. Message Bandwidth**

The message bandwidth required by the GMs is similar to that required by the FW Machines. A FDDI network interface provides 100 Mbits per second and easily covers any bandwidth requirements.

30 **1.5.11 DPC LAN**

1.5.11.1 Purpose

35 The DPC Local Area Network (LAN) links the machines of the DPC sites together using a fiber optic token ring. The fiber optic token ring provides both high bandwidth and good physical security.

1.5.11.2 Security

5 The network interfaces used by the machines on the DPC LAN include encryption hardware to make tapping or intercepting packets useless without the encryption key. The encryption key is the same for all machines on the LAN and is stored in the encryption hardware.

10 A properly configured network sniffer acts as an intruder detector as backup for the FW. If an anomalous message is detected, the intruding messages are recorded in their entirety, an operator is alerted, and the FW is physically shut down by the sniffer.

1.5.12 Message Processing Module

1.5.12.1 Purpose

15 The Message Processing Module (MPM) handles the processing for a request packet. It communicates with other components of the DPC as necessary to perform its tasks. The presence of an MPM on a machine brands it as a GM.

1.5.12.2 Usage

25 The MPM maintains a request context for each request it is currently processing. The request context includes the information necessary to maintain the network connection to the terminal making the request, the BIA device information, the response key, and the response packet.

1.5.13. Message Authentication Code Module

1.5.13.1. Purpose

30 The Message Authentication Code Module's (MACM) tasks are to validate the Message Authentication Code on inbound packets and to add a Message Authentication Code to outbound packets.

1.5.13.2. Usage

The MACM maintains an in-memory hash table of 112-bit MAC encryption keys keyed by BIA hardware identification code.

5 When the MACM receives a request from the GM to validate a packet's MAC, it first looks up the packet's hardware identification code in the hash table. If no entry exists, then the MACM replies to the GM with an "invalid hardware identification code" error.

10 Otherwise, the MACM performs a MAC check on the BIA message part of the packet using the 112-bit MAC encryption key. If the MAC check fails, then the MACM replies to the GM with an "invalid MAC" error. Otherwise, the MACM replies with a "valid MAC" message.

15 If the packet contains a merchant code, the MACM also checks the merchant code against the owner identification code in the hash table. If the codes don't match, then the MACM replies with an "invalid owner" error.

20 When the MACM receives a request from the GM to generate a MAC for a packet, it looks up the MAC encryption key using the packet's hardware identification code. With the MAC encryption key, the MACM generates a MAC and adds it to the packet. If the MACM cannot find the hardware identification code in its hash table, it replies with an invalid hardware identification code error instead.

1.5.13.3. Database Schema

25 The MACM hash table entry contains:

MACM Entry:

hardwareId = int4

ownerId = int4

macEncryptionKey = int16

30 The table is hashed by hardware identification code.

1.5.13.4. Database Size

5 Assuming 5 million BIA-equipped devices in service, the hash table requires about 120 MB of storage. For performance reasons, this hash table is cached completely in memory.

1.5.13.5. Dependencies

10 The MACM only contains records referencing active BIA hardware identification codes and active apparatus owners. Whenever an apparatus or apparatus owner is suspended or deleted from the system, the MACM removes any entries that reference the identification code. When an apparatus is activated, the MACM then adds an entry for it.

15 The MACM also caches the MAC encryption key from the Valid Apparatus Database. Since the system does not allow the encryption key of an BIA to be changed, the MACM does not need to worry about receiving encryption key updates.

1.5.14. Message Decrypt Module

1.5.14.1. Purpose

20
25 The Message Decrypt Module's (MDM) task is to reconstruct the DUKPT transaction key and with it decrypt the biometric- PIC block of the packet. It maintains a list of the DUKPT Base Keys that are required to generate the transaction key.

1.5.14.2. Usage

30 The MDM constructs the DUKPT transaction key using the packet's sequence number as the DUKPT transaction counter, the upper 22 bits of the BIA hardware identification code as the DUKPT tamper resistant security module (or "TRSM") Identification, and the low 10 bits of the BIA hardware identification code as the DUKPT Key Set Identification.

35 The DUKPT standard specifies how the transaction key is generated. The Key Set Identification is used to look up a Base Key from the

Base Key List. The Base Key is used to transform the TRSM Identification into the initial key via a DES encrypt/decrypt/encrypt cycle. The transaction counter is then applied to the initial key as a series of DES encrypt/decrypt/encrypt cycles to generate the transaction key.

For additional security, two Base Key Lists are maintained, one for low security BIA devices and one for high security devices. The MDM chooses which Base Key List to use depending on the security level of the device.

1.5.14.3. Database Schema

The MDM Base Key List entry contains:

MDM Entry:

baseKey = int16

The Base Key List is indexed by Key Set Identification.

1.5.14.4. Database Size

The MDM maintains an in-memory list of the DUKPT Base Keys. Each key requires 112-bits. The MDM maintains two sets of 1024 keys requiring 32 KB total.

1.5.14.5. Dependencies

The MDM has no direct dependencies on any other DPC component.

1.5.15. PIC Group List

1.5.15.1. Purpose

The PIC Group List (PGL), in conjunction with the Individual Biometric Database Machine List, defines the configuration of the IBD machines. The PGL stores a list of the PIC groups in the system which is used to simplify the management of the PICs. A PIC group is a set of consecutive PIC codes. A PGL exists on each GM Machine (GM).

1.5.15.2. Usage

5 The PGL, when given a PIC code, searches through its list of PIC groups for the group containing the PIC code. The PGL maintains the list of groups in order and uses a binary search to quickly find the correct group.

10 The initial configuration for the PGL is one giant PIC group containing all possible PICs. After a threshold number of PICs are assigned, the giant PIC group is split in two. Thereafter, this process is applied to all succeeding PIC groups.

15 When a PIC group splits, the PGL assigns a new main and backup IBD machine based on available storage on a first-come-first serve basis. The PGL coordinates with the IBD machines to first copy the affected records from the old main and backup machines to the new ones, update the IML record, and last remove the old main and backup copies. Splitting a PIC group is an involved task. The PGL batches split requests to be run when the DPC is lightly loaded, for instance, at night.

20 The system administrator may also change the main and backup IBD machines for a given PIC group if the machines' free storage falls below a level required for handling the expected amount of new registrations.

1.5.15.3. Database Schema

25 The schema for the PIC Group records are:

PICGroup:

lowPin = int8

highPin = int8

used = int4

30 Each PIC group is identified by a unique identifier. For convenience the PIC group identification code is the lowPin code for the group, however the system does not otherwise rely upon this fact.

35 The PGL is keyed by the lowPin field.

1.5.15.4. Database Size

5 The PGL is expected to contain about 3000 groups (each PIC group contains about 1000 active PICs, but may span millions of actual PICs). The entire PGL requires about 72 KB of storage and is cached completely in memory.

1.5.15.5. Dependencies

10 When PIC groups are added, merged, or split up, the PGL is responsible for informing the IBD Machine List of the changes and for directing the movement of IBD records from one IBD machine to another.

1.5.16. Individual Biometric Database Machine List

1.5.16.1. Purpose

15 The IBD Machine List (IML), in conjunction with the PIC Group List, codifies the configuration of the IBD machines. The IML maps a PIC code to the main and backup IBD machines storing IBD records for the PIC. The IML is actually keyed by PIC Group (a set of consecutive PIC codes) rather than by individual PICs because this greatly reduces the memory required to store the list. An IML exists on each GM Machine (GM).

1.5.16.2. Usage

20 When a GM processes a request that requires a biometric identification, the GM finds the IML record keyed by the biometric's PIC group. The GM then knows the main and backup IBD machines to use for the biometric identification.

25

30

1.5.16.3. Database Schema

The schema for the IML list entries are:

MachinePair:

pinGroup = int8

main = int2,

backup = int2

The IML is keyed by pinGroup.

1.5.16.4. Database Size

The IML is expected to contain about 3000 entries (the number of PIC Groups). Each MachinePair record is 12 bytes requiring about 36 KB of storage and is cached completely in memory.

1.5.16.5. Dependencies

Any changes in the configuration of the IBD machines are be reflected in the IML. In addition, the IML uses PIC groups for its keys so when the PIC Group List gets modified, the IML are also updated.

1.5.17. Sequence Number Module

1.5.17.1. Purpose

The Sequence Number Module's (SNM) primary function is to prevent replay attacks by validating packet sequence numbers. Its secondary task is to minimize the effects of a resubmission attack by informing other SNMs in remote DPC sites of sequence number updates and to periodically update the sequence numbers in the Valid Apparatus Database.

The SNM maintains an in-memory hash table of sequence numbers keyed by BIA hardware identification code codes to allow quick validation of packet sequence numbers.

1.5.17.2. Usage

5 When the SNM receives a validate request from the GM for a given hardware identification code and sequence number, it looks up the hardware identification code in the hash table. If no entry exists, then the SNM replies to the GM with an "invalid hardware identification code" error.

10 Otherwise, the SNM checks the given sequence number against the sequence number stored in the hash table entry. If the sequence number is less than or equal to the stored sequence number, the SNM replies with an "invalid sequence number" error. Otherwise, the SNM sets the sequence number in the hash table entry to the given sequence number and replies with a "valid sequence number" message.

15 From time to time, the SNM may observe a sequence number gap. A sequence number gap occurs when the SNM receives a sequence number that is more than one greater than the sequence number stored in the hash table entry. In other words, a sequence number was skipped. When the SNM discovers a sequence number gap, it replies with a "sequence number gap" message to the GM instead of a "valid sequence number" message. The GM treats the packet as valid, but it also logs a "sequence number gap" warning.

20 Sequence number gaps usually occur when network connectivity is lost: packets are dropped or can't be sent until the network is restored to working order. However, sequence number gaps occur for fraudulent reasons as well: malicious parties could intercept packets preventing them from arriving at the DPC or they could even attempt to counterfeit packets (with a large sequence number so that it isn't immediately rejected).

25 The SNM's secondary function is to inform other DPCs of the updated sequence numbers. Quickly updating sequence numbers at all DPC sites thwarts resubmission attacks wherein a malicious entity monitors packets whose destination is for one DPC site and immediately sends a copy to a different DPC site in the hope of exploiting the transmission delay of sequence number updates from one DPC site to another resulting in both sites accepting the packet as valid, when only the first site should accept the packet.

30 The SNMs send update messages to each other whenever they receive a valid sequence number. If an SNM receives an update message for a sequence number that is less than or equal to the sequence number currently

stored in its hash table, that SNM logs a sequence number resubmission warning. All resubmission attacks are detected in this manner.

5 A simpler way to thwart resubmission attacks completely, is to have only one SNM validate packets. Under this scheme, there is no update transmission delay window to exploit with a resubmission attack. Alternately, multiple SNMs can be active at the same time provided none of them handle sequence number validation for the same BIA-equipped device.

10 1.5.17.3. Sequence Number Maintenance

When the SNM boots up, it loads the sequence number hash table from the sequence numbers for active BIA stored in the VAD.

Once per day, the SNM downloads the current sequence numbers to the local Valid Apparatus Database (VAD).

15 The VAD is responsible for sending add-entry and remove-entry messages to the SNMs for any BIA-equipped devices that are activated or deactivated to keep the SNM hash table up-to-date.

20 1.5.17.4. Database Schema

The SNM hash table entry contains:

SNM Entry:

hardwareId = int4

sequenceNumber = int4

25 The hash table is keyed by hardwareId.

30 1.5.17.5. Database Size

Assuming about 5 million BIA-equipped devices in service requires the hash table to be about 40 MB.

1.5.17.6. Dependencies

5 The SNM depends on the Valid Apparatus Database. When an apparatus is suspended or removed from the database, the SNM removes the corresponding entry. When an apparatus is activated, the SNM creates an entry for it.

1.5.17.7. Message Bandwidth

10 The SNMs require a transmission bandwidth of about 8 KB per second to handle 1000 update sequence number messages per second. The update sequence number messages is buffered and sent out once per second to minimize the number of actual messages sent.

1.5.18. Apparatus Owner Database

1.5.18.1. Purpose

20 The Apparatus Owner Database (AOD) stores information on individuals or organizations that own one or more BIA-equipped devices. This information is used to double check that the BIA devices are used only by their rightful owners, to provide asset account information for financial credit and debit transactions, and to allow identification of all BIAs owned by a specific individual or organization.

1.5.18.2. Usage

30 Each AOD record includes an asset account to credit or debit the owner when the DPC processes a financial transaction submitted by one of the owner's BIA-equipped devices. For instance, transactions submitted from BIA attached to a retail point of sale terminal involves credits to the asset account, while certified electronic mail transmissions results in debits to the asset account.

1.5.18.3. Database Schema

The schema for the Apparatus Owner record is:

ApparatusOwner:

5 ownerId = int4
 name = char50
 address = char50
 zipCode = char9
 assetAccount = char16
10 status = int 1

The status field is one of:

0: suspended
1: active

15 The Apparatus Owner Database is keyed by ownerId.

1.5.18.4. Database size

20 The AOD is expected to store about 2 million Apparatus Owner
records. Each entry is 130 bytes requiring about 260 MB of storage. The AOD
is stored as a hashed file keyed by owner identification code. A copy of the
AOD is stored on each GM.

1.5.18.5. Dependencies

25 When entries are removed or suspended from the AOD, any Valid
Apparatus Database records that reference those apparatus owners are marked
as suspended. In addition, the MAC Module and the Sequence Number
Module remove their entries for the suspended apparatuses.

1.5.19. Valid Apparatus Database

1.5.19.1. Purpose

35 The Valid Apparatus Database (VAD) is a collection of records
representing all of the BIAs that have been manufactured to date. The VAD

record contains the Message Authentication Code encryption key for each BIA, as well as an indication of whether an BIA is active, awaiting shipment, or marked as destroyed. In order for a message from an BIA to be decrypted, the BIA must exist and have an active record in the VAD.

1.5.19.2. Usage

When manufactured, each BIA has a unique public identification code and a unique MAC encryption key, both of which are entered into the VAD record prior to BIA deployment.

When an BIA is first constructed, it is given a unique hardware identification code. When an BIA is placed in service, its hardware identification code is registered with the system. First, the owner or responsible party of the BIA is entered into the Apparatus Owner Database (AOD). Then, the VAD record is pointed to the AOD record, and the BIA is then set active. Requests from that BIA are accepted by the DPC.

When an BIA is removed from service, it is marked as inactive, and the link to the AOD record is broken. No communications from that BIA are accepted.

Each BIA type and model has a security level assigned to it that indicates its level of physical security. When the DPC processes requests from that BIA, it uses the BIA's security level to gauge what kind of actions are allowed. The DPC also provides the security level to external financial transaction authorization services.

For example, a financial transaction authorization service can decide to deny any request for over \$300 from low security BIA, requiring individuals to use higher security BIA to authorize such sums. The authorization service can also use the security level as a guide on how much to charge for the transaction, based on risk.

The security levels and the actions that they allow are determined operationally. Basically, the cost to defraud the system must be higher than the potential gain, so the security level is related to the cost to compromise the device.

1.5.19.3. Database Schema

The schema for the Valid Apparatus record is:

Valid Apparatus:

5 hardwareId = int4
macEncryptionKey = int16
ownerId = int8
mfgDate = time
inServiceDate = time
10 securityLevel = int2
status = int1
type = int1
use = int1

15 Possible values for the status field are:

0: suspended
1: active
2: destroyed

20 Possible values for the type field are (one for each type of terminal):

0: ATM
1: BRT
2: CET
3: CPT
25 4: CST
5: EST
6: IPT
7: IT
8: ITT
30 9: PPT
10: RPT
11: SFT

Possible values for the use field are:

0: retail

1: personal

2: issuer

3: remote

The Valid Apparatus Database is keyed by hardware identification code.

1.5.19.4. Database Size

The VAD handles about 5 million retail, issuer, and remote Valid Apparatus entries. Each entry is 51 bytes requiring about 255 MB total. The VAD is stored as a hashed file keyed by hardware identification code. A copy of the VAD is stored on each GM.

The number of personal Valid Apparatus entries number in the range of 30 million requiring another 1.5 GB of storage.

1.5.19.5. Dependencies

When a VAD record changes status, the MAC Modules and Sequence Number Modules are informed of its change in status. For instance, when an apparatus becomes active, the MACP and SNM adds an entry for the newly active apparatus. When an apparatus becomes inactive, the MACP and SNM remove their entry for the apparatus.

1.5.20. Individual Biometric Database

1.5.20.1. Purpose

Individual Biometric Database (IBD) records store information on individuals, including their primary and secondary biometrics, PIC code, list of financial asset accounts, private code, emergency account, address, and phone number. The individual may optionally include their SSN and electronic mail address. This information is necessary for identifying an individual either by biometric or personal information, for accessing account information, or for

providing an address or phone number to remote merchants for additional verification.

1.5.20.2. Usage

Individuals are added to the system during the individual enrollment process at registered Biometric Registration Terminals located in retail banking establishments worldwide, or in local system offices. During enrollment, individuals select their personal identification numbers, and add financial asset accounts to their biometric and PIC combination.

Individuals may be removed from the database due to fraudulent activity reported by any issuing member. If this occurs, the individual's account information is moved from the IBD to the Prior Fraud Database (PFD) by an authorized internal systems representative. The biometric Ids for records in the PFD may not be used for records in the IBD.

The IBD exists on multiple machines, each of which is responsible for a subset of the IBD records with a copy of each record stored on two different machines, both for redundancy and for load-sharing. The IBD Machine List, stored on the GM, maintains which machines hold which PICs.

1.5.20.3. Database Schema

The schema for the Individual Biometric record is:

IndividualBiometric:

```

primaryBiometric = biometric
secondaryBiometric = biometric
biometricId = int4
PIC = char10
phoneNumber = char12
lastName = char24
firstName = char24
middleInitial = char2
SSN = char9
privateCode = char40
address = char50
zipCode = char9

```

publicKey = char64
checksums = int4[10]
accountLinks = char30[10]
emergencyIndex = char1
5 emergencyLink = char1
privs = char10
enroller = int8
emergencyUseCount = int4
10 status = int1

The status field is one of:

- 0: suspended
- 1: active
- 15 2: priorFraud

The IBD is keyed by PIC.

1.5.20.4. Database Indexes

20 Each IBD machine has additional indexes on the individual's Social Security Number, biometric identification code, last name, first name, and phone number to facilitate access to the IBD database.

1.5.20.5. Database Size

25 Each IBD machine has 40 GB of secondary storage provided by one or more RAID devices. Each IBD record is 2658 bytes (assuming the biometrics are 1K apiece) allowing up to 15 million records per machine. The IBD records are stored using a (perhaps clustered) secondary index on the
30 PIC. The index is stored in memory and requires no more than 64 MB (a 64 MB index handles about 16 million entries). To store records for 300 million individuals, the DPC needs at least 40 IBD machines: 20 IBD machines for main storage and another 20 for backup. The number of IBD machines is easily scaled up or down depending on the number of registered individuals.
35

1.5.20.6. Dependencies

5 The IBD machines, PIC Group List, and the IBD Machine List remain up-to-date in terms of which PICs are on which machine. When a PIC group is reconfigured or main and backup machines for PIC groups are changed, the IBD machines update their databases and indexes appropriately.

1.5.21. Authorized Individual Database

10 1.5.21.1. Purpose

For each issuer or personal BIA-equipped device, the Authorized Individual Database (AID) maintains a list of individuals who are authorized, by the owner of the device, to use it.

15 The AID exists for two reasons. The first is that it provides restricted access to a terminal. For example, the Issuer Terminal can only be used by an authorized bank representative. The second reason for the AID is to prevent criminals from secretly replacing the BIA in a retail point of sale terminal with that of a personal BIA from a phone Terminal and thus routing all purchases to a remote merchant account set up by the criminals.

20 1.5.21.2. Database Schema

The schema for the Authorized Individual record is:

25 Authorized Individual:

hardwareId = int4

biometricId = int4

30 The hardwareId refers to a record in the Valid Apparatus Database and the biometricId refers to a record in the Individual Biometric Database. Whenever the DPC needs to check whether an individual is authorized to use a personal or issuer BIA device, the DPC checks for the existence of an Authorized Individual record with the correct hardwareId and biometricId.

35 Personal BIA devices are identified by a use field set to 1 (personal) in the Valid Apparatus Database. Issuer BIA devices are identified by a use field set to 2 (issuer) in the Valid Apparatus Database.

1.5.21.3. Database Size

5 Assuming each issuer terminal has 10 individuals authorized to use it and an each personal device has 2 additional authorized individuals with 1,000,000 personal devices in the server, the AID stores about:

$$10 * 100,000 + 2 * 1,000,000 = 3,000,000 \text{ entries}$$

10 The entire database requires about 24 MB of storage.

1.5.21.4. Dependencies

15 When Authorized Owner Database records or Valid Apparatus Database records are removed, all Authorized Individual records referencing them are removed.

1.5.22. Prior Fraud Database

1.5.22.1. Purpose

20 The Prior Fraud Database (PFD) is a collection of records representing individuals who have defrauded member issuers at some point in the past. The PFD also runs background transactions during periods of low system activity to weed out individuals in the IBD who have matching records in the PFD.

25 The system does not automatically put individuals in the PFD, unless it detects that they are attempting to register again. Placing an individual in the PFD is a sensitive policy matter which is outside the scope of this document.

1.5.22.2. Usage

30 Before a new IBD record is marked as active, the individual's primary and secondary biometrics are checked against each and every biometric in the PFD using the same biometric comparison techniques as those

used in the individual identification procedure.. If a match is found for the new IBD record, the IBD record's status is set to "prior fraud". If the prior fraud check was executed as part of a registration request, the GM logs a "registering individual with prior fraud" warning.

5 It is assumed that the PFD will remain relatively small. The cost to run the PFD is expensive, as it is an involuntary biometric search, so it is important to add only those individuals to the PFD who have imposed a significant cost to the system.

10 1.5.22.3. Database Schema

The schema for the Prior Fraud record is:

Prior Fraud:

15 primaryBiometric = biometric
 secondaryBiometric = biometric
 biometricId = int4
 PIC = char10
 phoneNumber = char12
 lastName = char24
 20 firstName = char24
 middleInitial = char2
 SSN = char9
 privateSignal = char40
 address = char50
 25 zipCode = char9
 publicKey = char64
 checksums = int4[10]
 accountLinks = char30[10]
 emergencyIndex = char1
 30 emergencyLink = char1
 privs = char10
 enroller = int8
 emergencyUseCount = int4
 35 status = int1

The status field is one of:

0: suspended

1: active

2: prior fraud

5

The PFD is keyed by biometric identification code.

1.5.22.4. Database Size

10

The PFD record is the same as the IBD record. Fortunately, the DPC needs to store a lot less of them so only two database machines are required to store the entire database, of which one is the backup.

1.5.22.5. Dependencies

15

The PFD does not have any direct dependencies on any other DPC component.

1.5.23. Issuer Database

20

1.5.23.1. Purpose

25

The Issuer Database (ID) stores information on banks and other financial institutions that allow their asset accounts to be accessed through the system. The issuing institutions are the only entities that can add or remove their asset account numbers to a given individual's IBD record.

1.5.23.2. Usage

30

The DPC uses the ID to validate requests from Issuer Terminals by searching the ID for a record containing the Issuer Terminal's issuer code. The owner Identification stored in the record must match up with the owner stored in the Valid Apparatus Database for the BIA stored in the Issuer Terminal.

The schema for the Issuer record is:

Issuer Record:

issuerCode = int6

ownerId = int4

name = char50

phoneNumber = char12

address = char50

zipCode = char9

The Issuer Database is keyed by issuerCode.

1.5.23.3. Database Size

The Issuer Database handles about 100,000 entries. Each entry is 127 bytes requiring less than 2 MB. A copy of the ID is stored on each GM.

1.5.23.4. Dependencies

The Issuer Database does not have any direct dependencies on any other DPC component.

1.5.24. Electronic Document Database

1.5.24.1. Purpose

The Electronic Document Database (EDD) stores and tracks electronic documents such as fax images and electronic mail messages destined for specified individuals. It also maintains corporate organizational charts to provide the official titles of both sender and receiver. The EDD also archives the documents at the sender or receiver's request and provides a neutral, third-party verification of contract agreements submitted through the system.

1.5.24.2. Usage

When the DPC receives a fax or other electronic document from an individual, it creates an EDD Document record to store the document until it is picked up by the authorized recipients.

For fax documents, the recipients are specified by fax number and extension. For other electronic documents, the recipients are specified by electronic mail address. The DPC looks up an Organization record for each recipient by fax number and extension or e-mail address. If the record cannot be found, then the DPC looks in the Individual Biometric Database but only if the recipient is specified by e-mail address. For each recipient, the DPC creates a Recipient record that references both the Document and the recipient's biometric Identification specified by the Organization or IBD record if found. The DPC allows recipients who are not registered in the system, but it cannot then ensure delivery or confidentiality for those recipients.

The EDD is flexible enough to allow fax documents to be sent to an individual's e-mail address and e-mail messages sent to a fax machine.

While no electronic signature is placed on the document by the system, the system does guarantee through encryption that the message as received (and decrypted) by the Certified Email or Secure Fax terminal was sent by the individual.

Duly authorized officers of the organization can submit secure faxes or electronic messages to the DPC to assign title and fax extensions to new members, to update a member's title or fax extension, or to remove terminated members.

When an individual is removed from the organization tree, the DPC retires the extension number for a period of one year. This retirement period allows the individual sufficient time to inform confidants that he can no longer receive confidential faxes at that extension and so that the organization cannot mistakenly activate someone else at the extension who might then otherwise receive faxes not intended for him or her.

The EDD maintains an archive database which contains copies of Document and Recipient records when requested by the sender or one of the recipients of the document. The archive database is periodically moved onto CD-ROM.

1.5.24.3. Database Schema

The EDD has three record types:

Document Record:

documentNumber = int8

senderId = int4

documentFax = fax

documentText = text

messageKey = int8

status = int1

Recipient Record:

documentNumber = int8

recipientId = int4

recipientFaxNumber = char12

recipientFaxExtension = char8

recipientEmailAddr = text

receivedBy = int4

lastModified = time

deliveryStatus = int1

contractStatus = int1

Archive Request Record:

biometricId = int4

documentNumber = int8

requestorFaxNumber = char12

requestorFaxExtension = char8

requestorEmailAddr = text

Organization Record:

biometricId = int4

registeredBy = int4

company = text

title = text

faxNumber = char12

faxExtension = char8

emailAddr = text

activeDate = time

privs = int2

status = int1

The Document record status field is one of:

0: incomplete

1: ok

The Recipient record delivery status field is one of:

0: incomplete

1: notified

2: rejected

3: retrieved

4: retrieved unsecured

5: busy

The Recipient record contract status field is one of:

0: none

1: accepted

2: rejected

The Organization record status field is one of:

0: active

1: suspended

The Organization record privs** field is used to indicate what privileges the DPC allows that individual:

0: registration

The Document, Recipient, and Archive Retrieve records are keyed by documentNumber. The Organization records are keyed by biometricId. The EDD maintains secondary indexes on the Document senderId field, the Recipient recipientId field, and the Organization company name and title fields.

1.5.24.4. Database Size

The EDD's storage requirements depend primarily on the number of fax pages it will have to store since e-mail messages are relatively small compared to fax pages. Each fax page requires about 110 KB of storage.

Assuming 4 pages per fax, 2 faxes per person per day, and 30 million fax machines, the EDD requires 24 GB of storage to spool one day's worth of faxes.

5 **1.5.24.5. Security**

Documents are sent to and from the system encrypted using the BIA encryption mechanism. However, the encryption key is stored in the same database as the document. The document is left in its encrypted form to
10 prevent casual disclosure, but individuals concerned about security of documents stored on the system should make some arrangement for additional encryption themselves.

15 **1.5.24.6. Message Bandwidth**

Each fax page requires about 110 KB which means that a T1 connection, with a throughput of 1.54 Mbits/second, can handle about 1.75 fax pages per second.

20 **1.5.25. Electronic Signature Database**

1.5.25.1. Purpose

25 The Electronic Signature Database (ESD) authenticates and tracks all electronic signatures created by the system.

1.5.25.2. Usage

30 Individuals who are members of the system submit a 16-byte "message digest" for the document along with biometric-PICs and obtain a "digital signature" which remains on file with the system in perpetuity. This digital signature encodes the individual's name, biometric identification code, the authorized signature record number, document title, along with the timestamp at which the document was signed.

To verify a signature, a message digest for the document are first calculated (using RSA's MD5 for instance) and sent along with the document's signature tags. The ESD looks up the signature tags and validates the just recently calculated message digest against the message digest stored in the database.

1.5.25.3. Database Schema

The schema for the Electronic Signature record is:

Electronic Signature:

signatureNumber = int8

signer = int4

documentName = text

checksum = int16

date = time

The signer is the biometric identification code for the individual signing the document. The electronic signature record is hashed by signatureNumber.

1.5.25.4. Database Size

For each 1 GB of secondary storage, the Electronic Signature Database stores 27 million records (each record is about 32 bytes).

1.5.25.5. Dependencies

The ESD has dependencies on the signer's biometric Identification. Since these signatures remain valid essentially forever, ESD records are not removed when the system deletes the signer's Individual Biometric Database record. Note that this requires the IBD to never reuse a biometric Identification.

1.5.26. Remote Merchant Database

1.5.26.1. Purpose

5 The Remote Merchant Database (RMD) stores information on
merchants that provide goods or services over telephones, cable television
networks, or the Internet. Each order sent by an individual using a
properly-equipped terminal is routed through the merchant's order terminal to
10 the system.

1.5.26.2. Usage

15 Once an individual's remote transaction authorization is received
and the MAC validated by the DPC, the merchant code is compared against
the merchant code in the RMD. The merchant code, be it phone number,
merchant-product credential, or internet address, exists in the RMD record
under the correct merchant identification code or the DPC terminates the
request and returns an invalid merchant code error to the sending BIA terminal
20 device.

1.5.26.3. Database Schema

The schema for the Remote Merchant record is:

Remote Merchant:

25 merchantId = int4
 merchantCode = char16
 merchantType = int1
 publicKey = int16

30 The Remote Merchant merchantType is one of:

 0: telephone
 1: CATV
 2: Internet

35 The merchantId and merchantCode are both primary keys. No two
RMD records have the same merchantId and merchantCode combination.

1.5.26.4. Database Size

5 Assuming about 100,000 remote merchants, the RMD requires about 24 bytes per record for a total of about 2.4 MB storage required.

1.5.26.5. Dependencies

10 The RMD does not have any direct dependencies on any other DPC components.

1.5.27. System Performance

15 The key performance number is how many financial authorization transactions the DPC handles per second.

In GM:

- 20
1. MACM checks the MAC (local)
 2. SNM checks the sequence number (network message)
 3. MDM decrypts the biometric-PIC block (local)
 4. Find IBD machine (local)
 5. Send identify request to the IBD machine (network message)

In IBD machine:

- 25
6. Retrieve all IBD records for the PIC (x seeks and x reads, where x is the number of pages required to store the biometric records).
 7. For each record, compare against its primary biometric ($y / 2$ ms where y is the number of records retrieved).
 - 30 8. If no reasonable match, repeat step 9 but compare against the secondary biometric ($z * y / 2$ ms, where y is the number of records retrieved and z is the probability no match is found).
 9. Update the best matching IBD record's checksum queue and check for possible replay attacks (1 seek, 1 read, and 1 write).

35

10. Return the best matching IBD record or an error if the match is not close enough (network message).

In GM:

5

- 11. Authorize request with an external processor (network message)
- 12. GM encrypts and MACs the response (local).
- 13. Sends response packet back (network message).

10

Total Disk Costs:

$$x * (s + r) + y / 2 * (1 + z) + s + r + w + 5 * n$$

$$= (x + 1) * (s + r) + y / 2 * (1 + z) + w + 5 * n$$

[assume x is 20, y is 30, z is 5%; s = 10ms, r = 0ms, w = 0ms, n = 0ms]

$$= 21 * 10 \text{ ms} + 15 * 1.05 \text{ ms}$$

15

$$= 226 \text{ ms}$$

$$= 4.4 \text{ TPS}$$

[assume x is 10, y is 15, z is 5%; s = 10ms, r = 0ms, w = 0ms, n = 0ms]

$$= 11 * 10 \text{ ms} + 7.5 * 1.05 \text{ ms}$$

$$= 118 \text{ ms}$$

20

$$= 8.4 \text{ TPS}$$

[assume x is 1, y is 1, z is 5%; s = 10ms, r = 0ms, w = 0ms, n = 0ms]

$$= 2 * 10 \text{ ms} + 1/2 * 1.05 \text{ ms}$$

$$= 21 \text{ ms}$$

25

$$= 47 \text{ TPS}$$

The backup IBD machine also processes requests doubling effective TPS.

Worst case (with 2 machines in use):

30

Individuals per PIC	TPS
30	8
15	16
1	94

Average case (with 20 machines in use):

Individuals per PIC	TPS
30	88
15	168
1	940

Best case (with 40 machines in use):

Individuals per PIC	TPS
30	176
15	336
1	1880

The above is just an example of one configuration of the system as it could be implemented in a commercially viable manner. However, it is anticipated that this invention can be configured in many other ways which could incorporate the use of faster computers, more computers and other such changes.

1.6. Terminal Protocol Flowchart

The following set of protocol flows describe interactions between specific terminals, the DPC, the attached BIA, and other parties such as the credit/debit processor, and so on.

1.6.1. Retail Point of Sale Terminal

In this case, an RPT communicates with a retail BIA and the DPC to authorize a transaction. The transaction amount is 452.33, the individual's account is 4024-2256-5521-1212 merchant code is 123456, and the individual's private code is "I am fully persuaded of it."

RPT → BIA Set Language <English>

BIA → RPT Ok

RPT → BIA Get Biometric <20>

BIA/LCD: <Please place finger on lighted panel>

Individual places finger on scanner

BIA → RPT Ok
 RPT → BIA Get Pin <40>
 BIA/LCD: <Please enter your PIC, then press <enter>>
 Individual enters PIC, then <enter>
 5 BIA → RPT Ok
 RPT → BIA Get Account Number <40>
 BIA/LCD: <Now enter your account index code, then press <enter>>
 Individual enters code, then <enter>
 BIA → RPT Ok
 10 RPT → BIA Validate Amount <452.33> <40>
 BIA/LCD: <Amount 452.33 OK?>
 Individual enters OK
 BIA → RPT Ok
 RPT → BIA Assign Register <1> <123456>
 15 BIA → RPT Ok
 RPT → Form Message <transaction>
 BIA → RPT <Transaction Request Message>
 BIA → RPT OK
 BIA/LCD: <I'm talking to DPC Central>
 20 RPT → DPC <Transaction Request Message>
 DPC: validate biometric, retrieve account number → 4024-2256- 5521-1212
 DPC → VISA <authorize 4024-2256-5521-1212 452.33 123456>
 VISA → DPC <ok 4024-2256-5521-1212 452.33 123456 autho-code>
 DPC: get private code
 25 DPC → RPT <Transaction Response Message>
 RPT → BIA Show Response <Transaction Response Message> <8>
 BIA/LCD: <Transaction ok: I am fully persuaded of it>
 BIA → RPT <Ok <autho-code>>
 RPT: prints receipt with autho-code on it
 30

1.6.2. Internet Point of Sale Terminal

In this case, an IPT communicates with a standard BIA and the DPC to authorize a transaction. The transaction amount is 452.33, the individual's account is 4024-2256-5521-1212, the internet merchant is located
 35

at merchant.com, his merchant code is 123456, and the individual's private code is "I am fully persuaded of it."

5 IPT → merchant.com <send me merchant code if resources available>

merchant.com → IPT <ok 123456 merchant.com-public-key>

IPT generates session key, encrypted with merchant.com-public-key

IPT → merchant.com <session key>

All subsequent communications with merchant are encrypted with session key.

10 merchant.com → IPT <price and product information>

IPT/Screen: displays price and product information

Individual: selects item "fruitcake, price 45.33"

IPT → BIA Set Language <English>

BIA → IPT Ok

IPT → BIA Get Biometric <20>

15 BIA/LCD: <Please place finger on lighted panel>

Individual places finger on scanner

BIA → IPT Ok

IPT → BIA Get Pin <40>

20 BIA/LCD: <Please enter your PIC, then press <enter>>

Individual enters PIC, then <enter>

BIA → IPT Ok

IPT → BIA Get Account Number <40>

BIA/LCD: <Now enter your account index code, then press <enter>>

Individual enters code, then <enter>

25 BIA → IPT Ok

IPT → BIA Validate Amount <45.33> <40>

BIA/LCD: <Amount 45.33 OK?>

Individual enters OK

BIA → IPT Ok

30 IPT → BIA Assign Register <1> <123456>

BIA → IPT Ok

IPT → BIA Assign Register <2> <merchant.com>

BIA → IPT Ok

IPT → BIA Assign Register <3> <fruitcake>

35 BIA → IPT Ok

IPT → BIA Form Message <remote transaction>

BIA → IPT <Remote Transaction Request Message>
 BIA → IPT OK
 BIA/LCD: <I'm talking to DPC Central>
 IPT → merchant.com <Remote Transaction Request Message>
 5 merchant.com → secure-connect to DPC using DPC public key
 merchant.com → DPC <Remote Transaction Request Message>
 DPC: validate biometric, retrieve account number → 4024-2256- 5521-1212
 DPC: validate internet merchant.com with code 123456
 DPC → VISA <authorize 4024-2256-5521-1212 45.33 123456>
 10 VISA → DPC <ok 4024-2256-5521-1212 45.33 123456 autho- code>
 DPC: get private code
 DPC → merchant.com <Transaction Response Message>
 merchant.com stores autho code
 merchant.com → IPT <Transaction Response Message>
 15 IPT → BIA Show Response <Transaction Response Message> <8>
 BIA/LCD: <Transaction ok: I am fully persuaded of it>
 BIA → IPT <Transaction ok>

1.6.3. Internet Teller Terminal

20 In this case, an ITT communicates with a standard BIA, the DPC,
 and a bank's internet server to perform routine and nonroutine home banking
 operations. Note that the DPC isn't involved in actually validating any
 transactions, but is only responsible for creating a valid set of network
 25 credentials and securing the communications line to the bank.

ITT → bank.com <send me bank code if resources available>
 bank.com → ITT <ok 1200>
 ITT → BIA Set Language <English>
 30 BIA → ITT Ok
 ITT → BIA Get Biometric <20>
 BIA/LCD: <Please place finger on lighted panel>
 Individual places finger on scanner
 BIA → ITT Ok
 35 ITT → BIA Get Pin <40>
 BIA/LCD: <Please enter your PIC, then press <enter>>

Individual enters PIC, then <enter>

BIA → ITT Ok

RPT → BIA Get Account Number <40>

BIA/LCD: <Now enter your account index code, then press <enter>>

5

Individual enters code, then <enter>

BIA → ITT Ok

ITT → BIA Assign Register <1> <1200> (bank code)

BIA → ITT Ok

ITT → BIA Assign Register <2> <bank.com>

10

BIA → ITT Ok

ITT → BIA Assign Register <3> <ITT.port, bank.com.port> (TCP/IP addresses)

BIA → ITT Ok

ITT → Form Message <net credential>

BIA → ITT <network credential Request>

15

BIA → ITT Ok

BIA/LCD: <I'm talking to DPC Central>

ITT → DPC <network credential Request>

DPC: validate biometric, create credential(time, acct, bank)

DPC: get private code

20

DPC → ITT <network credential Response>

ITT → BIA Show Response <network credential Response>

BIA decrypt response, check response

BIA/LCD: <Credential ok: I am fully persuaded of it>

BIA encrypt credential, session key, challenge key with bank's public key

25

BIA → ITT <Secure Connection Request Message>

BIA → ITT <Session Key>

BIA → ITT Ok

BIA/LCD: <Secure connection to bank.com in progress>

ITT → bank.com <Secure Connection Request Message>

30

bank.com decrypt with private key, validate credential, use shared key

bank.com → ITT <ok>

Further transactions over the ITT → bank.com connections are all encrypted by the ITT using the ITT/bank session key.

35

Any transactions that the bank determines are non-routine must be validated by the individual using the BIA's challenge-response mechanism.

The challenge-response mechanism is available only while the BIA remains in the "secure connection" state.

5 bank.com → ITT <validate <validation request>>
 ITT → BIA Validate Private <encrypted validation request>
 BIA decrypts challenge section, and displays it
 BIA/LCD: <Please OK: transfer of 12,420.00 to 1023-3302- 2101-1100>
 Individual enters Ok
 BIA re-encrypts response using challenge key
 10 BIA/LCD: <Secure connection to bank.com in progress>
 BIA → ITT <Ok <encrypted validation response>>
 ITT → bank.com <encrypted validation response>

1.6.4. Electronic Signature Terminal

15 In this case, an EST communicates with a standard BIA and the DPC to construct digital signatures. The individual's private code is "I am fully persuaded of it" and the document to be signed is called "The Letter of Marque."

20 CET → BIA Set Language <English>
 BIA → CET Ok
 CET → BIA Get Biometric <20>
 BIA/LCD: <Please place finger on lighted panel>
 25 Individual places finger on scanner
 BIA → CET Ok
 CET → BIA Get Pin <40>
 BIA/LCD: <Please enter your PIC, then press <enter>>
 Individual enters PIC, then <enter>
 30 BIA → CET Ok
 CET → BIA Validate Document <Letter of Marque> <40>
 BIA/LCD: <Document "Letter of Marque" OK?>
 Individual enters OK
 BIA → CET Ok
 35 CET → BIA Assign Register <1> <document MD5 value>
 BIA → CET Ok

CET → Form Message <signature submit>
 BIA → CET <Electronic Signature Request>
 BIA → CET OK
 BIA/LCD: <I'm talking to DPC Central>
 5 CET → DPC <Electronic Signature Request>
 DPC: validate biometric, create signature, return sig text code
 DPC: get private code
 DPC → CET <Electronic Signature Response>
 CET → BIA Show Response <Electronic Signature Response> <8>
 10 BIA/LCD: <Document ok: I am fully persuaded of it>
 BIA → CET <Ok <sig text code>>

1.6.5. Certified Email Terminal

15 In this case, a CET communicates with a standard BIA and the
 DPC to transmit certified electronic mail. The individual's private code is "I
 am fully persuaded of it", and the document name is "Post Captain."

20 CET → BIA Set Language <English>
 BIA → CET Ok
 CET → BIA Get Biometric <20>
 BIA/LCD: <Please place finger on lighted panel>
 Individual places finger on scanner
 BIA → CET Ok
 25 CET → BIA Get Pin <40>
 BIA/LCD: <Please enter your PIC, then press <enter>>
 Individual enters PIC, then <enter>
 BIA → CET Ok
 30 CET → BIA Validate Document <Post Captain> <40>
 BIA/LCD: <Document "Post Captain" OK?>
 Individual enters OK
 CET/Screen: <Recipient list? >
 Individual enters <fred@telerate.com joe@reuters.com>
 35 CET → BIA Assign Register <1> <fred@telerate.com joe@reuters.com>
 BIA → CET Ok
 CET → Form Message <document submit>

BIA → CET <Electronic Document Submit Request>

BIA → CET OK

BIA/LCD: <I'm talking to DPC Central>

CET → DPC <Electronic Document Submit Request>

5

DPC: validate biometric, create message, return message #001234

DPC: get private code

DPC → CET <Electronic Document Submit Response>

CET → BIA Show Response <Electronic Document Submit Response> <8>

BIA/LCD: <Document ok: I am fully persuaded of it>

10

BIA → CET <Document ok <1234>>

CET → DPC <Electronic Document Data Request, 1234, section 1, incomplete>

DPC → CET <Electronic Document Data Response, incomplete>

CET → DPC <Electronic Document Data Request, 1234, section 2, incomplete>

DPC → CET <Electronic Document Data Response, incomplete>

15

CET → DPC <Electronic Document Data Request, 1234, section 3, incomplete>

DPC → CET <Electronic Document Data Response, incomplete>

CET → DPC <Electronic Document Data Request, 1234, section 4, done>

DPC → CET <Electronic Document Data Response, track 1234.1 1234.2>

DPC → fred@telerate.com <email 1234.1 message arrived>

20

DPC → joe@reuters.com <email 1234.2 message arrived>

mailer@telerate.com → DPC <received notification email for 1234.1>

DPC → sender@company.com <email 1234.1 recipient notified>

mailer@reuters.com → DPC <received notification email for 1234.2>

DPC → sender@company.com <email 1234.2 recipient notified>

25

[At Fred's CET: Fred sees the "message arrived" electronic mail message, and decides to go pick up the message]

CET → BIA Set Language <English>

30

BIA → CET Ok

CET → BIA Get Biometric <20>

BIA/LCD: <Please place finger on lighted panel>

Individual places finger on scanner

BIA → CET Ok

35

CET → BIA Get Pin <40> BIA/LCD: <Please enter your PIC>

Individual enters PIC, then <enter>

BIA → CET Ok
 CET → BIA Assign Register <1> <1234.1>
 BIA → CET Ok
 CET → Form Message <document retrieve>
 5 BIA → CET <Electronic Document Retrieve Request>
 BIA → CET OK
 BIA/LCD: <I'm talking to DPC Central>
 CET → DPC <Electronic Document Retrieve Request>
 DPC: validate biometric, lookup 1234.1
 10 DPC: get private code
 DPC → CET <Electronic Document Retrieve Response>
 CET → BIA Show Response <Electronic Document Retrieve Response> <8>
 BIA/LCD: <Document ok: I am fully persuaded of it>
 BIA → CET <Document ok <message key>>
 15 CET/Screen: decrypt, then show document

1.6.6. Secure Fax Terminal

In this case, a SFT communicates with an BIA/catv and the DPC to
 20 transmit secure faxes.

SFT → BIA Get Biometric <20>
 BIA/LCD: <Please place finger on lighted panel>
 Individual places finger on scanner
 25 BIA → SFT Ok
 BIA/LCD: <Please enter your PIC, then press <enter>>
 Individual enters PIC, then <enter>
 SFT → BIA Set Pin <40>
 BIA/LCD: <Please enter your Title Index, then press <enter>>
 30 Individual enters title index, then <enter>
 SFT → BIA Set Title Index Code <40>
 BIA → SFT Ok
 SFT/Screen: <Recipient? (add * for ext, # at end)>
 Individual enters <1 510 944-6300*525#>
 35 SFT/Screen: <Recipient? (add * for ext, # at end)>
 Individual enters <1 415-877-7770#>

SFT/Screen: <Recipient? (add * for ext, # at end)>

Individual enters <#>

SFT → BIA Assign Register <1> <15109446300*525 14158777770>

BIA → SFT Ok

5 SFT → Form Message <document submit>

BIA → SFT <Secure Fax Submit Request>

BIA → SFT OK

BIA/LCD: <I'm talking to DPC Central>

SFT → DPC <Secure Fax Submit Request>

10 DPC: validate biometric, create message, return message #001234

DPC: get private code

DPC → SFT <Secure Fax Submit Response>

SFT → BIA Show Response <Secure Fax Submit Response> <10>

BIA/LCD: <Document ok: I am fully persuaded of it>

15 BIA → SFT <Document ok <001234>>

SFT → DPC <Secure Fax Data Request, 1234, section 1, incomplete>

DPC → SFT <Secure Fax Data Response, incomplete>

SFT → DPC <Secure Fax Data Request, 1234, section 2, incomplete>

DPC → SFT <Secure Fax Data Response, incomplete>

20 SFT → DPC <Secure Fax Data Request, 1234, section 3, incomplete>

DPC → SFT <Secure Fax Data Response, incomplete>

SFT → DPC <Secure Fax Data Request, 1234, section 4, done>

DPC → SFT <Secure Fax Data Response>

DPC → connect-fax 15109446300

25 DPC → SFT6300 <fax-cover "Sam Spade" from "Fred Jones" 1234.1 4 pages waiting>

DPC → disconnect

DPC → connect-fax 14158777770

DPC → SFT7770 <fax-cover "John Jett" from "Fred Jones" 1234.2 4 pages waiting>

DPC → disconnect

30

[At Sam's SFT: Sam sees document fax cover arrive from Fred, initiates retrieval of document from DPC using tracking code 1234.1.]

SFT → BIA Get Biometric <20>

35 BIA/LCD: <Please place finger on lighted panel>

Individual (Sam) places finger on scanner

BIA → SFT Ok
 SFT → BIA Get Pin <40>
 BIA/LCD: <Please enter your PIC, then press <enter>>
 Individual (Sam) enters PIC, then <enter>
 5 BIA → SFT Ok
 SFT → BIA Assign Register <1> <1234.1>
 BIA → SFT Ok
 SFT → Form Message <document retrieve>
 BIA → SFT <Secure Fax Retrieve Request>
 10 BIA → SFT OK
 BIA/LCD: <I'm talking to DPC Central>
 SFT → DPC <Secure Fax Retrieve Request>
 DPC: validate biometric, lookup 1234.1, verify biometric-PIC = Sam Spade
 DPC: lookup private code in database
 15 DPC → SFT <Secure Fax Retrieve Response>
 SFT → BIA Show Response <Secure Fax Retrieve Response> <8>
 BIA → SFT <Document ok: I am fully persuaded of it <message key>>
 SFT/Screen: <Document ok: I am fully persuaded of it>
 SFT/Screen: print fax
 20

1.6.7. Biometric Registration Terminal

In this case, a BRT communicates with a registration BIA and the DPC to register an individual with the system.

25 BRT → BIA Set Language <English>
 BIA → BRT Ok
 BRT → BIA Get Biometric <20> <primary>
 BIA/LCD: <Please place PRIMARY finger on lighted panel>
 30 Individual places primary finger on scanner
 BIA → BRT Ok
 BRT → BIA Get Biometric <20> <secondary>
 BIA/LCD: <Please place SECONDARY finger on lighted panel>
 Individual places secondary finger on scanner
 35 BIA → BRT Ok
 BRT → BIA Get Pin <40>

BIA/LCD: <Please enter your PIC, then press <enter>>
Individual enters 123456, then <enter>
BIA → BRT Ok
BRT → BIA Get Message Key
5 BIA → BRT <Ok <message key>>
BIA → <Registration Request Message>
BRT/Screen: <Name: >
Representative enters <Fred G. Shultz>
BRT/Screen: <Address: >
10 Representative enters <1234 North Main>
BRT/Screen: <Zipcode: >
Representative enters <94042>
BRT/Screen: <Private code: >
Representative queries individual, then enters <I am fully persuaded of it.>
15 BRT/Screen: <Asset account list: >
Representative enters <2, 1001-2001-1020-2011> (credit card)
Representative enters <3, 1001-1002-0039-2212> (checking account)
BRT/Screen: <Emergency account: >
20 Representative enters <1, 1001-1002-0039-2212> (emergency, checking
account)
BRT → Form Message <registration>
BIA → BRT <Registration Request Message>
BIA → BRT OK
BIA/LCD: <I'm talking to DPC Central>
25 BRT appends message-key-encrypted personal information to request
BRT → DPC Registration Request Message> <encrypted personal information>
DPC: verify PIC 123456
DPC → BRT <Registration Response Message>
BRT → BIA Show Response <Registration Response Message> <8>
30 BIA/LCD: <Registration ok: I am fully persuaded of it, 123456>
BIA → BRT <Ok>

1.6.8. Customer Service Terminal

In this case, a CST communicates with a standard BIA and the DPC to verify the identity and the credentials of an individual.

5

CST → BIA Set Language <English>

BIA → CST Ok

CST → BIA Get Biometric <20>

BIA/LCD: <Please place finger on lighted panel>

10

Individual places finger on scanner

BIA → CST Ok

CST → BIA Get Pin <40>

BIA/LCD: <Please enter your PIC, then press <enter>>

Individual enters PIC, then <enter>

15

BIA → CST Ok

CST → BIA Get Message Key

BIA → CST <Ok <message key>>

CST → Form Message <Individual Identity Request>

20

BIA → CST <Individual Identity Request>

BIA → CST OK

BIA/LCD: <I'm talking to DPC Central>

CST → DPC <Individual Identity Request>

DPC: get private code, individual's priv

25

DPC → CST <Individual Identity Reply>

CST → BIA Show Response <Individual Identity Reply> <8>

BIA/LCD: <Identity ok: I am fully persuaded of it>

BIA → CST <Ok <individual-name priv>>

30

CST: check priv to see if sufficient for CST use

1.6.9. Issuer Terminal

In this case, an IT communicates with a standard BIA and the DPC to authorize and send a batch of account addition and deletion requests to the DPC. The individual's private code is "I am fully persuaded of it", and the bank code is 1200.

35

IT → BIA Set Language <English>
 BIA → IT Ok
 IT → BIA Get Biometric <20>
 5 BIA/LCD: <Please place finger on lighted panel>
 Individual places finger on scanner
 BIA → IT Ok
 IT → BIA Get Pin <40>
 BIA/LCD: <Please enter your PIC, then press <enter>>
 10 Individual enters PIC, then <enter>
 BIA → IT Ok
 IT → BIA Assign Register <1> <1200>
 BIA → IT Ok
 IT → BIA Get Message Key
 15 BIA → IT <message key>
 BIA → IT Ok
 IT → BIA Form Message <issuer request>
 BIA → IT <Issuer Batch Request>
 BIA → IT OK
 20 BIA/LCD: <I'm talking to DPC Central>
 IT → DPC <Issuer Batch Request> <message-key-encrypted issuer batch>
 DPC: validate biometric, validate bank code 1200 vs. BIA identification
 DPC: get private code
 DPC: decrypt message using message key, execute issuer batch
 25 DPC → IT <Issuer Batch Reply>
 IT → BIA Show Response <Issuer Batch Reply> <8>
 BIA/LCD: <Batch ok: I am fully persuaded of it>
 BIA → IT <Ok>

30 1.6.10. Automated Teller Machinery

In this case, an ATM communicates with an integrated ATM BIA
 and the DPC to identify an individual and obtain his bank account number.
 The individual's account is 2100-0245-3778-1201, bank code is 2100, and the
 35 individual's private code is "I am fully persuaded of it."

ATM → BIA Get Biometric <20>
 ATM/LCD: <Please place finger on lighted panel>
 Individual places finger on scanner
 BIA → ATM Ok
 5 ATM/LCD: <Please enter your PIC, then press <enter>>
 Individual enters 123456 on ATM keyboard, then <enter>
 ATM → BIA Set Pin <123456>
 BIA → ATM Ok
 ATM/LCD: <Now enter your account index code, then press <enter>>
 10 Individual enters 2, then <enter>
 ATM → BIA Set Account Index Code <2>
 BIA → ATM Ok
 ATM → BIA Assign Register <1> <2100>
 BIA → ATM Ok
 15 ATM → Form Message <account access>
 BIA → ATM <Account Access Request Message>
 BIA → ATM OK
 ATM/LED: <I'm talking to DPC Central>
 ATM → DPC <Account Access Request Message>
 20 DPC: validate biometric, retrieve account number →2100- 0245-3778-1201
 DPC: get private code
 DPC → ATM <Account Access Response Message>
 ATM → BIA Decrypt Response <Account Access Response Message>
 BIA → ATM <2100-0245-3778-1201> <no emergency> <I am fully persuaded of it>
 25 ATM/LCD: <I am fully persuaded of it>

At this point, the ATM has the account number it needs to continue, so it then retrieves the information associated with the account number, and commences interacting with the individual.

1.6.11. Phone Point of sale Terminal

In this case, a PPT communicates with an integrated phone BIA and the telephone merchant to download information and purchase items securely using the telephone. The individual's PIC is 1234, the account index

code is 1, the merchant's phone number is 1 800 542-2231, merchant code 123456, and the actual account number is 4024-2256-5521- 1212.

Note that the telephone strips the area code (1-800) from the telephone number before handing it to the system.

Individual dials phone 18005422231

PPT → connect merchant 18005422231

PPT → BIA Assign Register 1 <5422231>

Sales rep answers. Individual selects item "fruitcake". Sales rep downloads info.
merchant → PPT <123456 fruitcake 43.54>

PPT → BIA Get Biometric <20>

Phone/LCD: <Please place finger on lighted panel>

Individual places finger on scanner

BIA → PPT Ok

Phone/LCD: <Please enter your PIC, then press #>

Individual enters 1234 on keypad, then # or * (enter)

PPT → BIA Set Pin <1234>

BIA → PPT Ok

Phone/LCD: <Now enter your account index code>

Individual enters 1, then <enter>

RPT → BIA Set Account index code <1>

BIA → PPT Ok

RPT → BIA Assign Register <2> <123456>

BIA → PPT Ok

Phone/LCD: <Press # if amount 45.54 is ok>

Individual enters # (yes)

PPT → BIA Set Amount <43.54>

BIA → PPT Ok

PPT → Form Message <remote transaction>

BIA → PPT <Remote Transaction Request>

BIA → PPT Ok

Phone/LCD: <I'm talking to DPC Central>

PPT → merchant <Phone Transaction Request>

merchant → DPC secure-connect to DPC using DPC-public-key

merchant → DPC <Phone Transaction Request>

DPC: validate biometric, retrieve account number → 4024- 2256-5521-1212

DPC: validate merchant 5422231 has code 123456

DPC → VISA <authorize 4024-2256-5521-1212 43.54 123456>

VISA → DPC <ok 4024-2256-5521-1212 43.54 123456 autho- code>

DPC: get private code

DPC → merchant <Transaction Response Message>

merchant examines response code

merchant → PPT <Transaction Response Message>

PPT → BIA Decrypt Message <Transaction Response Message>

BIA → PPT <Ok <I am fully persuaded of it> <autho-code>>

Phone/LCD: <chime> Transaction ok: I am fully persuaded of it

1.6.12. Cable-TV Point of sale Terminal

In this case, a CPT communicates with an integrated cable-tv BIA and the Cable television merchant to download information and purchase items securely using the cable television broadband network. The individual's PIC is 1234, the account index code is 1, the channel is 5, the merchant code 123456, and the actual account number is 4024-2256-5521- 1212.

Individual turns the television to channel 5.

merchant → CPT <fruitcake 43.54 123456> (broadcast)

Individual hits "buy" on TV Remote

CPT/TV: <Buying fruitcake for \$43.54>

CPT → BIA Get Biometric <20>

CPT/TV: <Please place finger on lighted panel>

Individual places finger on scanner

BIA → CPT Ok

CPT/TV: <Please enter your PIC, then press <enter>>

Individual enters 1234 on keypad, then "buy"

CPT → BIA Set Pin <1234>

BIA → CPT Ok

CPT/TV: <Now enter your account index code>

Individual enters 1, then <enter>

RPT → BIA Set Account index code <1>

BIA → CPT Ok

RPT → BIA Assign Register <1> <channel 5, 15:30:20 PST>
 BIA → RPT Ok
 CPT → BIA Assign Register <2> <123456>
 BIA → CPT Ok
 5 CPT/TV: <Press "buy" if amount 45.54 is ok>
 Individual enters "buy"
 CPT → BIA Set Amount <43.54>
 BIA → CPT Ok
 CPT → Form Message <CableTV transaction>
 10 BIA → CPT <CableTV Transaction Request>
 BIA → CPT Ok
 CPT/TV: <I'm talking to DPC Central>
 CPT → CTV Center <CableTV Transaction Request>
 CTV Center → merchant <CableTV Transaction Request>
 15 merchant → DPC secure-connect to DPC using DPC-public-key
 merchant → DPC <CableTV Transaction Request>
 DPC: validate biometric, retrieve account number → 4024-2256- 5521-1212
 DPC: validate merchant channel 5, current show has code 123456
 DPC → VISA <authorize 4024-2256-5521-1212 43.54 123456>
 20 VISA → DPC <ok 4024-2256-5521-1212 43.54 123456 autho- code>
 DPC: get private code, mailing address
 DPC → merchant <Transaction Response Message>
 merchant examines response code, records mailing address
 merchant → CTV Center <Transaction Response Message>
 25 CTV Center → CPT <Transaction Response Message>
 CPT → BIA Decrypt Message <Transaction Response Message>
 BIA → CPT <Ok <I am fully persuaded of it> <autho-code>>
 CPT/TV: <chime> Transaction ok: I am fully persuaded of it

30 From the foregoing, it will be appreciated how the objects and
 features of the invention are met.

35 First, the invention provides a computer identification system that
 eliminates the need for a user to possess and present a physical object, such as
 a token, in order to initiate a system access request.

Second, the invention provides a computer identification system that is capable of verifying a user's identity, as opposed to verifying possession of proprietary objects and information.

5 Third, the invention verifies the user's identity based upon one or more unique characteristics physically personal to the user.

Fourth, the invention provides an identification system that is practical, convenient, and easy use.

10 Fifth, the invention provides a system of secured access to a computer system that is highly resistant to fraudulent access attempts by non-authorized users.

Sixth, the invention provides a computer identification system that enables a user to notify authorities that a particular access request is being coerced by a third party without giving notice to the third party of the notification.

15 Seventh, the invention provides an identification system that allows for identification of the sender and recipient of an electronic message and/or facsimile.

20 Although the invention has been described with respect to a particular tokenless identification system and method for its use, it will be appreciated that various modifications of the apparatus and method are possible without departing from the invention, which is defined by the claims set forth below.

5. GLOSSARY

ACCOUNT INDEX CODE:

5

A digit or an alpha-numeric sequence that corresponds to a particular financial asset account

AID:

10

Authorized Individual Database: contains the list of individuals authorized to use personal and issuer BIA devices.

AOD:

Apparatus Owner Database: central repository containing the geographic and contact information on the owner of each BIA.

15

ASCII:

American Standard Code for Information Interchange

ATM:

20

Automated Teller Machinery; uses encoded biometric identity information to obtain access to a financial asset management system, including cash dispensing and account management.

BIA:

25

Biometric input apparatus; collects biometric identity information, encodes and encrypts it, and makes it available for authorizations. Comes in different hardware models and software versions.

Biometric:

30

A measurement taken by the system of some aspect of an individual's physical person.

Biometric ID:

35

An identifier used by the system to uniquely identify an individual's biometric record (IRID – Individual Record ID)

BIO-PIC GROUP:

A collection of algorithmically dissimilar biometric samples linked to the same personal identification code

BRT:

Biometric Registration Terminal; located at retail banking outlets, BRTs combine biometric registration information with an individual-selected PIN and selected personal information to register individuals with the system.

CBC:

Cipher Block Chaining: an encryption mode for the DES.

CCD:

Charged-Coupled Device

CET:

Certified Email Terminal; uses BIA to identify sender, encrypts document, sends to system. System retains, notifies recipient of message arrival in-system. Recipient identifies self, and then document is transmitted to recipient. Notification to transmitter once document is sent. Document is verified sent, secured by BIA encryption. Transmitter may inquire as to delivery status. Both participants must be system members.

COMMANDS:

A program or subroutine residing in the DPC that performs a specific task, activated by a request message sent from a BIA-equipped terminal.

CONTRACT ACCEPT/REJECT:

The process by which an individual enters their BIO-PIC and instructs the DPC to register said individual's contractual acceptance or rejection of the terms contained within a document which had been sent by electronic facsimile to that individual.

CPT:

5 Cable-TV Point-of-Sale Terminal: combines an onscreen display simulcast digital signal informing TV-top cable box of product information with product video, and an BIA controller remote which performs the biometric-pin validation using the CATV communications network. Order/autho/mailling-address/item-id forwarded to merchant. Results of authorization are displayed on the TV.

CST:

10 Customer Service Terminals; provide system customer service personnel with varying degrees of access (based on access privilege) the ability to retrieve and modify information on individuals in order to help people with account problems.

DATA SEALING STEP:

15 The conversion of plain text to cipher text (known as "encryption") in combination with the encrypted checksumming of a message that allows information to remain in plain text while at the same time providing a means for detecting any subsequent modification of the message.

DES:

20 Digital Encryption Standard: a standard for the cryptographic protection of digital data. See standard ANSI X3.92-1981

DETERMINATION:

25 The status of the command processed during the execution step.

DPC:

30 A data processing center, namely, the place and the entity where the hardware, software, and personnel are located with the goal of supporting a multigigabyte biometric identity database. A DPC processes electronic messages, most of which involve performing biometric identity checks as a precursor to performing some action, such as a financial transfer, or sending a fax, or sending
35 electronic mail, etc.

DSP:

Digital Signal Processor: a class of integrated circuits that specialize in the mathematical operations required by the signal processing applications.

5

DUKPT:

Derived Unique Key Per Transaction: See standard ANSI/ABA X9.24-1992

10

EDD:

Electronic Document Database: central repository containing all pending faxes and electronic messages awaiting pickup by individuals.

15

EMERGENCY ACCOUNT INDEX:

The alpha-numeric digit or sequence selected by an individual which, when accessed, will result in a transaction being labeled by the system as an emergency transaction, potentially causing the display of false screens and/or the notification of authorities that said individual has been coerced into performing a transmission or transaction.

20

ESD:

Electronic Signature Database: central repository containing all MD5 and electronic signatures of all documents signed by anybody, referenced by authorization number.

25

EST:

Electronic Signature Terminal; uses BIA to identify individual, computer calculates checksum on document, sends checksum to system, system validates, timestamps, saves checksum, and returns with sig code. Uses Internet as transport. EST also verifies signatures given a sig code and an MD5 calculation.

30

FAR (False Accept Rate):

The statistical likelihood that one individual's biometric will be incorrectly identified as the biometric of another individual.

35

FALSE SCREENS:

5 Displays of information which has been intentionally pre- determined to be subtly inaccurate such that a coercing party will not illegally obtain accurate data about an individual's financial assets, all the while remaining unaware of the alteration of the information.

FDDI:

10 Fiber Digital Device Interface: a networking device that utilizes a fiber optic token ring.

FS:

Field Separator

FW:

15 Firewall Machine: the internet-local net router that regulates traffic into and out of the DPC.

GM:

20 Gateway Machine: the main processing computers in the DPC; runs most of the software.

IBD:

25 Individual Biometric Database: central repository for biometric, financial asset, and other personal information. Queries against the biometric database are used to verify identity for transaction authorizations and transmissions.

ID:

30 Issuer Database: central repository containing the institutions that are allowed to add and delete financial asset account numbers with the system.

IML:

35 IBD Machine List: a software module in the DPC determines which IBD machines are responsible for which PIN codes.

INTERNET MERCHANT:

A retail account selling services or good to consumers by means of the Internet electronic network

IPT:

Internet Point-of-Sale Terminal: items and merchant code from the internet, BIA biometric-PIN for validation, sent to system using Internet, autho/order/PO # forwarded to merchant. System response using internet as well, displaying results on screen.

ISSUER:

A financial account issuer for financial assets to be registered with the DPC.

ISSUER BATCH:

A collection of "add" and "delete" instructions complete with biometric IDs, financial asset accounts, and account index codes verified and submitted by an issuer to the DPC.

IT:

Issuer Terminals; provides a batch connection to the system for issuers to add and remove (their own) financial asset account numbers from specific individual's IBD records.

ITT:

Internet Teller Terminal; authorizes network terminal session using encrypted credential obtained from DPC using biometric ID.

LCD:

Liquid Crystal Display: a technology used for displaying text.

MAC:

Message Authentication Code: an encrypted checksum algorithm, the MAC provides assurance that the contents of a message have not been altered subsequent to the MAC calculation. See standard ANSI X9.9-1986

5

MACM:

Message Authentication Code Module: a software module in the DPC that handles MAC validation and generation for inbound and outbound packets.

10

MDM:

Message Decrypt Module: a software module in the DPC that encrypts and decrypts packets from or destined to an BIA device.

15

MPM:

Message Processing Module: a software module in the DPC that performs the processing of request packets.

20

NETWORK CREDENTIAL:

Both the individual and the bank are identified by the DPC to create the network credential. The credential includes the individual's identification as well as the context of the connection (i.e., the TCP/IP source and destination ports). DPC creates a network credential using the individual's account id, the time of day, and the bank code. The DPC signs this credential using Public Key Encryption and the DPC's Private Key.

25

PFD:

Prior Fraud Database: central repository for IBD records which have had prior fraud associated with them. Every new customer's biometrics are checked against all PFD records with the intent of reducing recidivism.

30

PGL:

PIN Group List: a software module in the DPC that is responsible for maintaining the configuration of the IBD machines.

35

PIN:

Personal Identification Number; a method for protecting access to an individual's account through secret knowledge, formed from at least one number.

5

PIC:

Personal Identification Code; a PIN formed from either numbers, symbols, or alphabetic characters.

10

POS:

Point-Of-Sale; a place where goods are sold.

PPT:

Phone Point-of-Sale Terminal; combines phone number with merchant price and product information to authorize a transaction over a BIA-equipped telephone. Order/authorization/mailling-address/PO forwarded to merchant. Resulting authorization is displayed on phone LCD, or "spoken", along with the individual's private code.

15

20

RAM:

Random Access Memory

RF:

Radio Frequency: generally refers to radio frequency energy emitted during the normal operation of electrical devices.

25

REGISTERS:

Memory reserved for a specific purpose, data set aside on chips and stored operands to instructions

30

REQUESTS:

Electronic instructions from the BIA to DPC instructing the DPC to identify the individual and thereby process the individual's command in the event the identification is successful

35

RMD:

Remote Merchant Database: contains all merchant identification codes for merchant telephone and Cable TV order shops; indexed by merchant ID. Contains per-merchant system encryption codes as well.

5

RPT:

Retail Point-of-Sale Terminal; combines encoded biometric identity information with retail transaction information (possibly from an electronic cash register) and formulates authorization requests of the system using X.25 networks, modems, etc.

10

SECURE TRANSMISSION:

An electronic message or facsimile wherein at least one party has been identified by the DPC.

15

SFT:

Secured Fax Terminal; uses BIA to identify sender, sends fax either unsecured, sender-secured, secured, or secured-confidential. The latter two require recipients to identify themselves using biometric-PIN. Uses "titles" (specified using a title index digit) to label outbound faxes. Sender may inquire as to delivery status. Both participants must be system members. Either sender or recipient can request that the fax be archived.

20

25

SNM:

Sequence Number Module: a software module in the DPC that handles the DUKPT sequence number processing for inbound request packets. Sequence number processing protects against replay attacks.

30

Terminal:

A device that uses the BIA to collect biometric samples and form request messages that are subsequently sent to the DPC for authorization and execution. Terminals almost always append ancillary information to request messages, identifying counterparties and the like.

35

TITLE INDEX CODE:

Alpha-numeric sequence uniquely identifying an individual's authorized role or capacity within the context of his employment

Token:

An inanimate object conferring a capability.

TRACKING CODE:

An alpha-numeric sequence assigned to data stored in or transmitted by the DPC, such that said sequence may be used to recall the data or obtain a report on the status of the transmission of the data.

TRANSACTION:

An electronic financial exchange

TRANSMISSION:

An electronic message other than an electronic financial exchange

VAD:

Valid Apparatus Database: central repository in which each BIA (with associated unique encryption codes) is identified, along with the owner of the BIA.

I claim:

1. A voluntary tokenless identification computer system for determining an individual's identity from an examination of at least one biometric sample and a personal identification code gathered during a bid step, and comparison with previously recorded biometric sample and personal identification code gathered during a registration step, said system comprising:
 - a. at least one computer;
 - b. first gathering and display means for voluntary input of at least one biometric sample, personal identification code, and private code from an individual during the registration step, wherein the private code is selected by the individual;
 - c. second gathering and display means for voluntary input of at least one biometric sample and personal identification code, from an individual during a bid step;
 - d. first interconnecting means for interconnecting said first and second gathering and display means to said computer for transmitting the gathered biometric sample, personal identification code, and private code from said first and second gathering means to said computer;
 - e. means for comparison of biometric sample and personal identification code gathered during the bid step with the biometric sample and personal identification code gathered during the registration step, for producing an evaluation;
 - f. execution means within said computer for storage of data and processing and execution of commands for producing a determination; and
 - g. means for output of said evaluation, determination, or private code from said computer.
2. The apparatus of claim 1 wherein the computer comprises means for detecting and preventing electronic intrusion of the computer system.
3. The apparatus of claim 1 wherein the computer is placed remote from the gathering and display means.
4. The apparatus of claim 1, the first and second gathering and display means further comprising:
 - a. at least one biometric input means for gathering biometric samples further comprising a hardware and software component;
 - b. at least one terminal means that is functionally partially or fully integrated with the biometric input means for input of and appending additional data;

- 5
6. c. at least one data entry means for input of a personal identification code where in said means is integrated either with the biometric input means or the terminal means; and
7. d. second interconnecting means for interconnecting said biometric input means, data entry means and said terminal.
8. 5. The apparatus of claim 4 wherein said terminal further comprises at least one display means for display of data.
9. 6. The apparatus of claim 4 wherein the biometric input means has a hardware identification code previously registered with the computer, which makes the biometric input means uniquely identifiable to the computer.
10. 7. The apparatus of claim 4 wherein the hardware component further comprises:
11. a. at least one computing module for data processing;
12. b. erasable and non-erasable memory modules for storage of data and software;
13. c. biometric scanner device for input of biometrics data;
14. d. data entry means for entering data;
15. e. digital communication port; and
16. f. means for prevention of electronic eavesdropping.
17. 8. The apparatus of claim 7 wherein the computing modules are connected in a manner to prevent monitoring of communications between said computing modules.
18. 9. The apparatus of claim 7 wherein the hardware component further comprises display means for display of data.
19. 10. The apparatus of claim 7 wherein the hardware component further comprises RF shielding .
20. 11. The apparatus of claim 4 wherein the hardware component further comprises a wireless communications means.
21. 12. The apparatus of claim 7 wherein the biometric input means is secured from physical tampering.
22. 13. The apparatus of claim 12 further comprising means for detection of physical penetration of the biometric input means.
23. 14. The apparatus of claim 13 further comprising means for electronic self destruction whereby software and data stored within the memory module are erased.
24. 15. The apparatus of claim 13 further comprising means for physical self destruction whereby the computing modules and memory modules are destroyed.
25. 16. The apparatus of claim 4 wherein the hardware component further comprises means for reading magnetic strip cards.
- 30
- 35

17. The apparatus of claim 4 wherein the hardware component further comprises means for reading a smart card.
18. The apparatus of claim 4 wherein the software component resides in a computing module and further comprises;
- 5 a. electronically erasable memory module wherein at least one command interface module, a first set of software and associated data specifically configured for the intended use of the biometric input device and data are stored; and
- b. non-erasable memory module wherein a second set of software and
- 10 associated data are stored.
19. The apparatus of claim 18 said software component further comprising means for encryption of data from plaintext to ciphertext.
20. The apparatus of claim 18 said software component further comprising means to detect alteration of data further comprising;
- 15 a. a secret key; and
- b. an irreversible one way transformation of the data that cannot be reproduced without the secret key.
21. The apparatus of claim 18 wherein the first set of software and associated data further comprising:
- 20 a. biometric encoding algorithm; and
- b. encryption code.
22. The apparatus of claim 18 wherein the second set of software and associated data further comprising:
- 25 a. an operating system; and
- b. at least one device driver.
23. The apparatus of claim 4 wherein said terminal is any electronic device and which issues commands to and receives results from the biometric input means.
24. The apparatus of claim 23 wherein said terminal is selected from the group of facsimile machines, telephones, television remote control, personal computers, credit/debit card
- 30 processors, cash registers, automated teller machines, wireless personal computers.
25. The apparatus of claim 4 wherein said second interconnecting means is means for wireless communications.
26. The apparatus of claim 1 wherein said first interconnecting means is selected from the group X.25, ATM network, Telephone network, Internet network, cable television
- 35 network, cellular telephone network.

27. The apparatus of claim 1 wherein the comparison means further comprises means for encryption and decryption of data.
28. The apparatus of claim 1 wherein comparison means further comprises means for identifying the biometric input device.
- 5 29. The apparatus of claim 1 wherein the computer system further comprises:
- a. at least one independent computer network system; and
 - b. third interconnecting means for interconnecting said computer system with said counter party computer system.
- 10 30. The apparatus of claim 29 wherein the third interconnecting means comprises an X.25 network.
31. The apparatus of claim 1 wherein the execution means comprises at least one database for storage and retrieval of data.
32. The apparatus of claim 31 wherein the data base further comprises an individual biometric data base.
- 15 33. The apparatus of claim 31 wherein the data base further comprises a prior fraud check data base.
34. The apparatus of claim 31 wherein the data base further comprises an electronic document data base.
- 20 35. The apparatus of claim 31 wherein the data base further comprises an electronic signature data base.
36. The apparatus of claim 1 wherein said output means is selected from the group of an X.25 network, ATM network, Telephone network, Internet network, cable television network.
- 25 37. The apparatus of claim 1 wherein said private code is generated by the computer.
38. A method for voluntary and tokenless identification of individuals, and authentication of the identification, said method comprising the steps of:
- a. registration step wherein at least one biometric sample, personal identification code, and private code from an individual is gathered and stored;
 - 30 b. bid step wherein at least one biometric sample and personal identification code from an individual is gathered;
 - c. comparison step wherein the biometric sample and personal identification code gathered during the bid step is compared with the biometric sample and personal identification code gathered and stored during the registration step, for producing either a successful or failed identification result;
- 35

- d. execution step wherein a command is processed and executed to produce a determination;
 - e. output step wherein said identification result or determination is externalized and displayed; and
 - 5 f. presentation step wherein on successful identification of the individual, the private code is presented to the individual being identified.
39. The method of claim 38 wherein both the registration and bid steps further comprise a biometric sample check step wherein the quality of the biometric sample is verified.
- 10 40. The method of claim 38 wherein the registration step further comprises a personal identification code and biometric sample duplication check step wherein the biometrics and personal identification code gathered during the registration step is checked against all previously registered biometrics currently associated with the identical personal identification code.
- 15 41. The method of claim 38 wherein the registration step further comprises an ancillary data input step wherein ancillary data is collected.
42. The method of claim 41 wherein the ancillary data further comprises name and address of the individual.
43. The method of claim 41 wherein the ancillary data further comprises a title of an individual.
- 20 44. The method of claim 43 wherein the ancillary data input step further comprises a title index assignment step wherein each title of the individual is assigned a code.
45. The method of claim 41 wherein the ancillary data further comprises a financial asset account number.
- 25 46. The method of claim 45 wherein the ancillary data input step further comprises an account index assignment step wherein each financial asset account number is assigned an index code.
47. The method of claim 38 wherein the registration step further comprises a prior fraud check step wherein the biometric sample gathered during registration is compared to a subset of previously registered biometric samples.
- 30 48. The method of claim 38 wherein the registration step further comprises an emergency mechanism setup step.
49. The method of claim 48 further comprising an emergency account index assignment step wherein an account index is labeled as an emergency account where in the event the account is accessed appropriate authorities are notified of the emergency.
- 35 50. The method of claim 49 further comprising a false screen display setup step wherein there is assignment of false screen data.

51. The method of claim 49 wherein access to various financial asset accounts is limited.
52. The method of claim 38 wherein the registration step further comprises a modification step wherein any previously entered ancillary data can be modified or deleted.
53. The method of claim 38 wherein both the registration and bid steps further comprise a
5 data sealing step to provide the ability to detect alteration of the data further comprising;
- a. a secret key; and
 - b. an irreversible one way transformation of the data that cannot be reproduced without the secret key.
54. The method of claim 38, wherein the registration and bid steps further comprise an
10 encryption step to convert the data from plaintext to ciphertext.
55. The method of claim 38 wherein the bid or registration steps further comprise a transmission step wherein the data is transmitted.
56. The method of claim 38 wherein the bid or registration steps is further provided with a
15 unique transmission code having a unique hardware identification code and incrementing sequence number which increases by one for each transmission.
57. The method of claim 38 wherein the registration step further comprises choosing a language for communication in a set language step.
58. The method of claim 38 wherein the bid step further comprises choosing a title in a set
20 title number step.
59. The method of claim 38 wherein the bid step further comprises choosing an account number in a set account number step.
60. The method of claim 38 wherein the bid step further comprises validating an amount in a validate amount step.
61. The method of claim 38 wherein the bid step further comprises entering an amount in
25 an enter amount step.
62. The method of claim 38 wherein the bid step further comprises validating a document in a validate document step.
63. The method of claim 38 wherein the bid step further comprises appending ancillary
30 data in an assign register step.
64. The method of claim 63 the ancillary data further comprising a counter party identification code.
65. The method of claim 38 wherein the bid or registration step further comprise aborting or canceling said step in a reset step.
66. The method of claim 38 wherein the bid step further comprises transmission of data in
35 a transmission step.

- 5 67. The method of claim 38 wherein the bid step further comprises choosing a language for communication in a set language step.
68. The method of claim 38 wherein the comparison step further comprises use of the unique transmission codes to detect repeat transmissions.
- 5 69. The method of claim 38 wherein the comparison step further comprises a counter party identification step using the counter party identification and unique transmission codes.
- 10 70. The method of claim 38 wherein the comparison step comprises matching the individual's personal identification code and biometric gathered during the bid step, with the personal identification code and biometric gathered during the registration step for positive identification of the individual.
71. The method of claim 70 wherein if there is no match of the personal identification code and biometric gathered during the registration step and the personal identification code and biometric gathered during the bid step, there is no recognition of the individual.
- 15 72. The method of claim 38 wherein the execution step further comprises a debit/credit transaction step.
73. The method of claim 72 wherein the debit/credit transaction step further comprises an address collection step.
- 20 74. The method of claim 38 wherein the execution step further comprises an archiving step and a tracking code assignment step for archival of data.
75. The method of claim 74 wherein the data is sent through a message digest encoding algorithm step to produce an electronically signed document.
76. The method of claim 38 wherein the execution step further comprises the retrieval of archived data using said tracking code.
- 25 77. The method of claim 38 wherein the execution step further comprises a modification step wherein the title index code, account numbers and account index codes are added, deleted or modified.
78. The method of claim 38 wherein the execution step further comprises an account number retrieval step where the account index code is used to retrieve an account number.
- 30 79. The method of claim 38 wherein the execution step further comprises an emergency activation step.
80. The method of claim 79 wherein the emergency activation step further comprises recognition of the emergency code and identifying the entire transaction as an emergency and notification of authorities.
- 35

81. The method of claim 79 wherein the execution step further comprises a false display step wherein previously designated, false accounts or false limitations on accounts are accessible.
82. The method of claim 38 wherein the output step further comprises an identification result notification step.
83. The method of claim 38 wherein the output step further comprises a determination notification step.
84. The method of claim 38 wherein the output step further comprises an emergency code step wherein authorities are notified.
85. The method of claim 38 wherein the output step further comprises display of false screens.
86. The method of claim 38 wherein the presentation step further comprises encryption, externalization, and decryption of the private code.
87. A method for rapid search of at least one first previously stored biometric sample from a first individual, using a personal identification code-basket that is capable of containing at least one algorithmically unique second biometric sample from at least one second individual, and which is identified by said personal identification code-basket, comprising:
- a. a storage step further comprising:
 - i. selection of a personal identification code by said first individual;
 - ii. entering a biometric sample from said first individual;
 - iii. locating the personal identification code-basket identified by the personal identification code selected by said first individual;
 - iv. comparison of the biometric sample taken from said first individual, with any previously stored biometric samples in said selected personal identification code-basket, to make sure that the biometric sample entered by said first individual is algorithmically unique from the previously stored at least one biometric sample provided by at least one second individual; and
 - v. storage of the entered biometric sample from said first individual in the selected personal identification code-basket if said sample is algorithmically unique from the at least one previously stored biometric sample from said at least one second individual; and
 - b. a bid step further comprising:
 - i. entering said selected personal identification code by said first individual; and

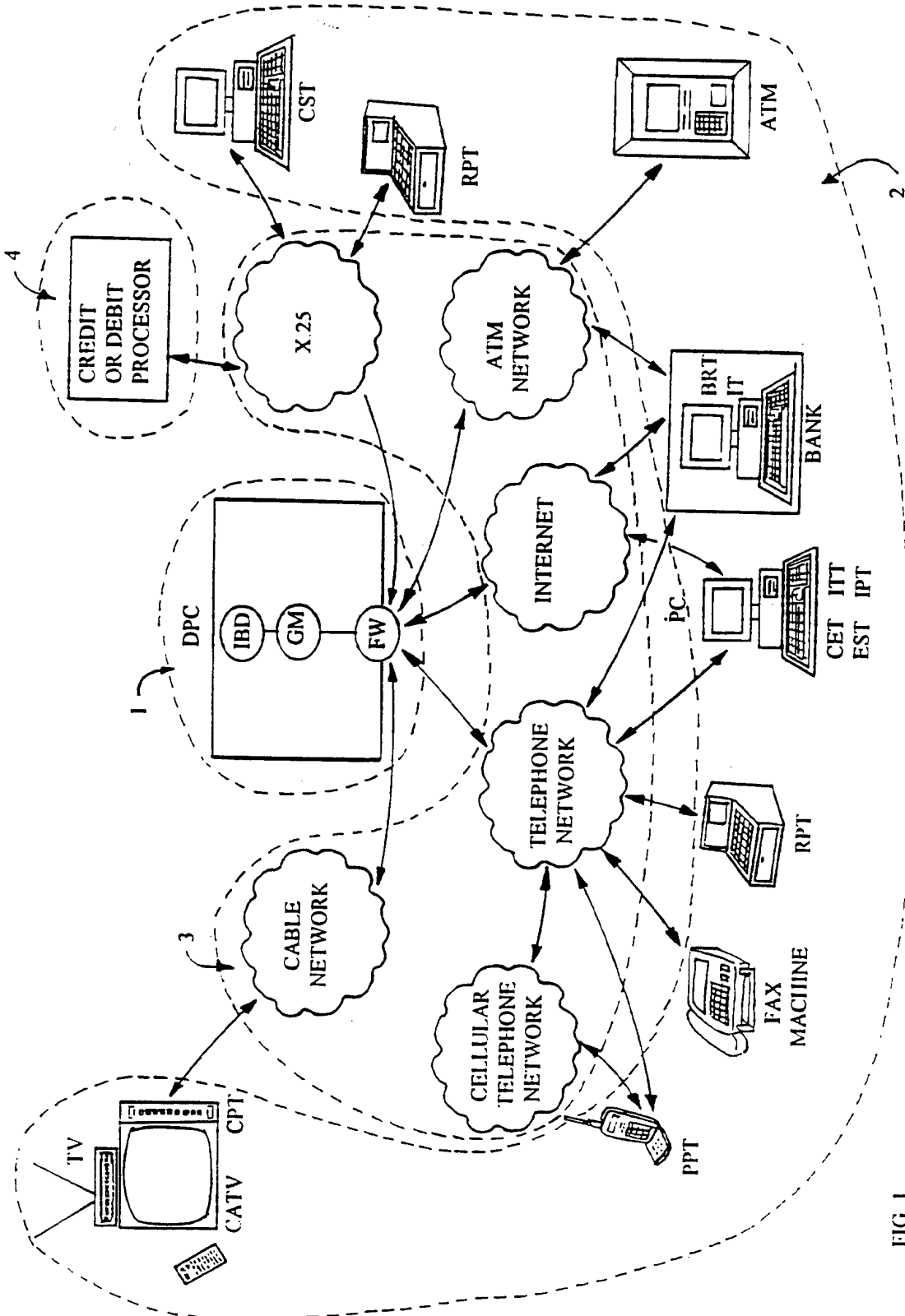


FIG. 1

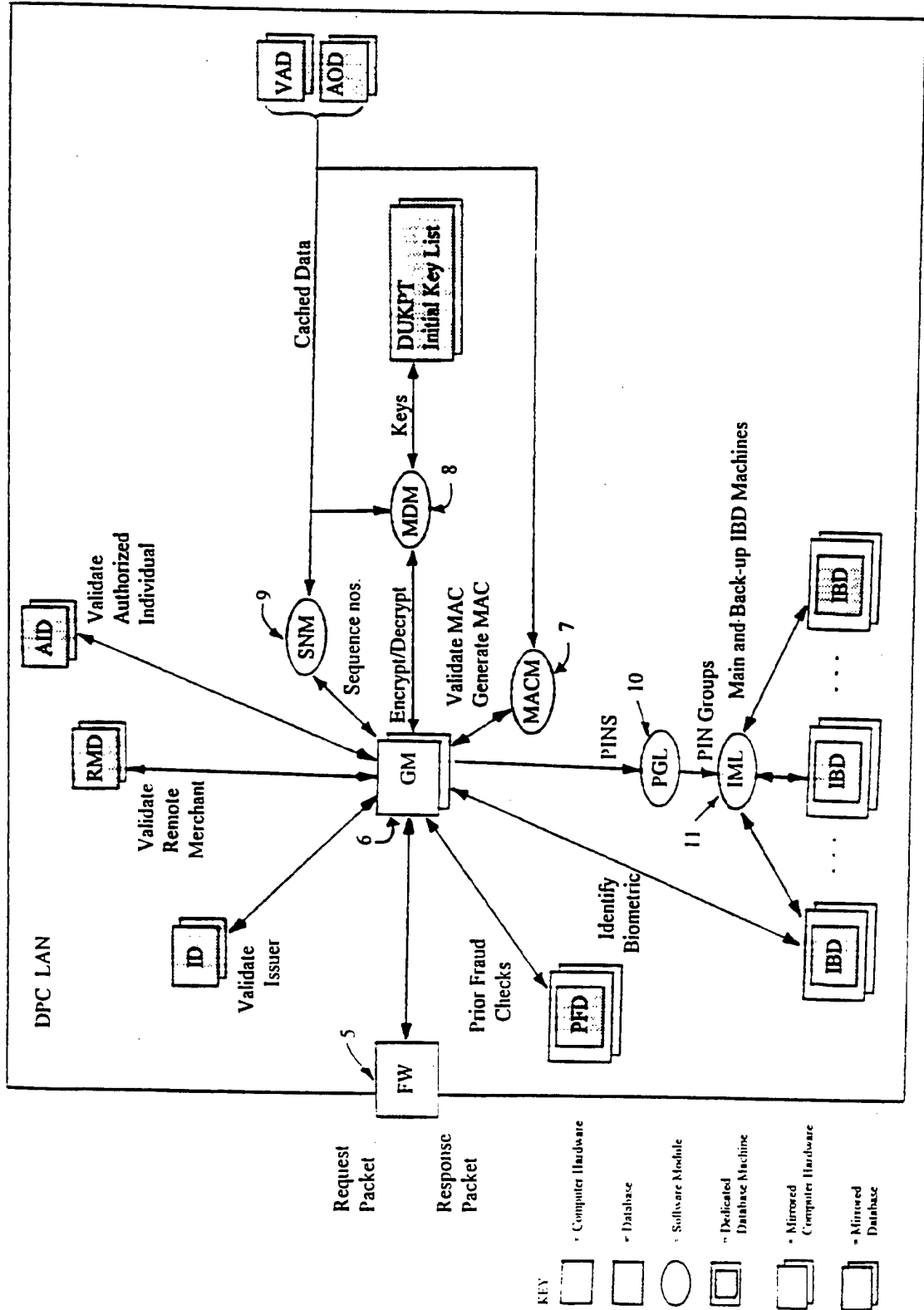


FIG. 2

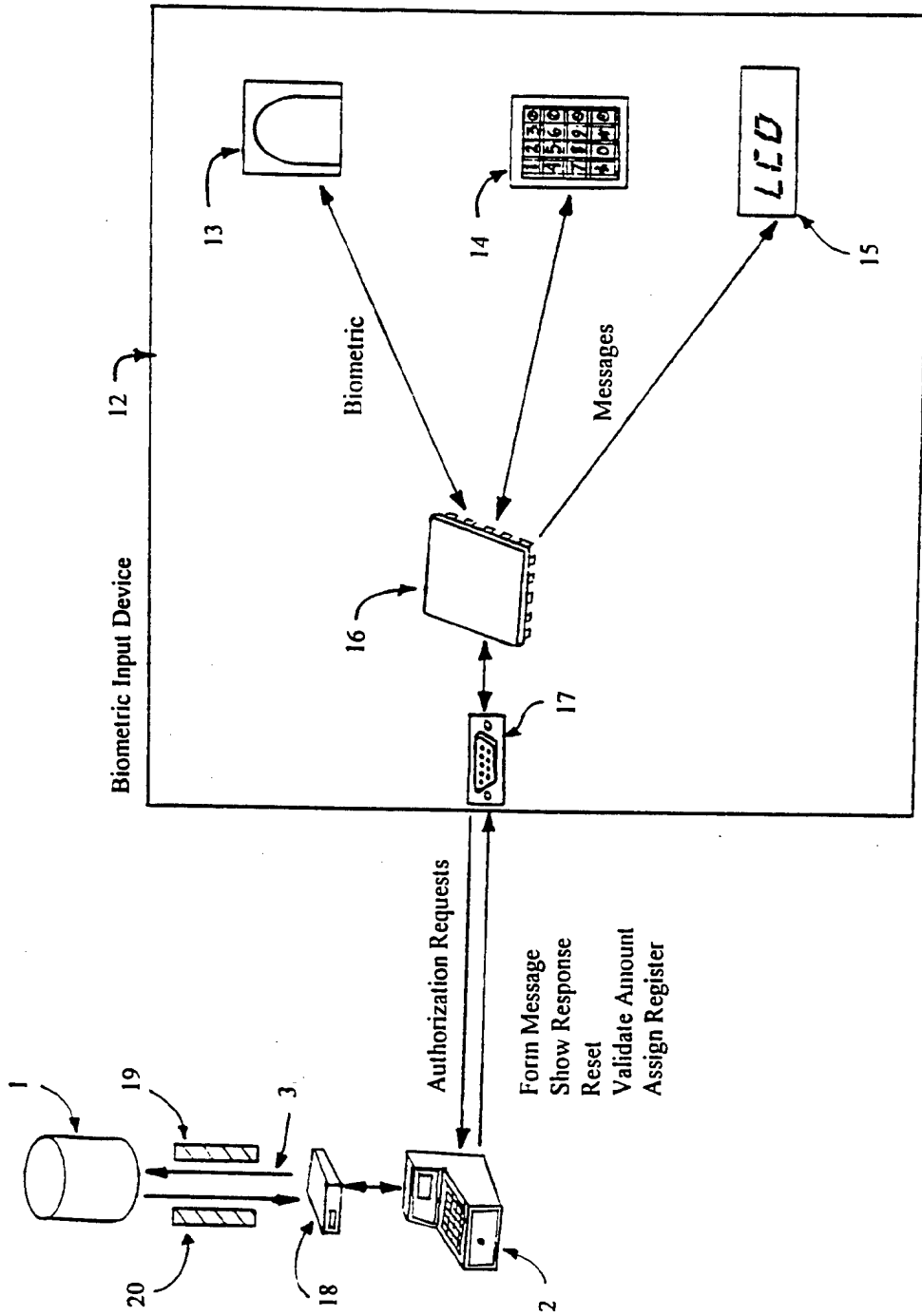


FIG. 3

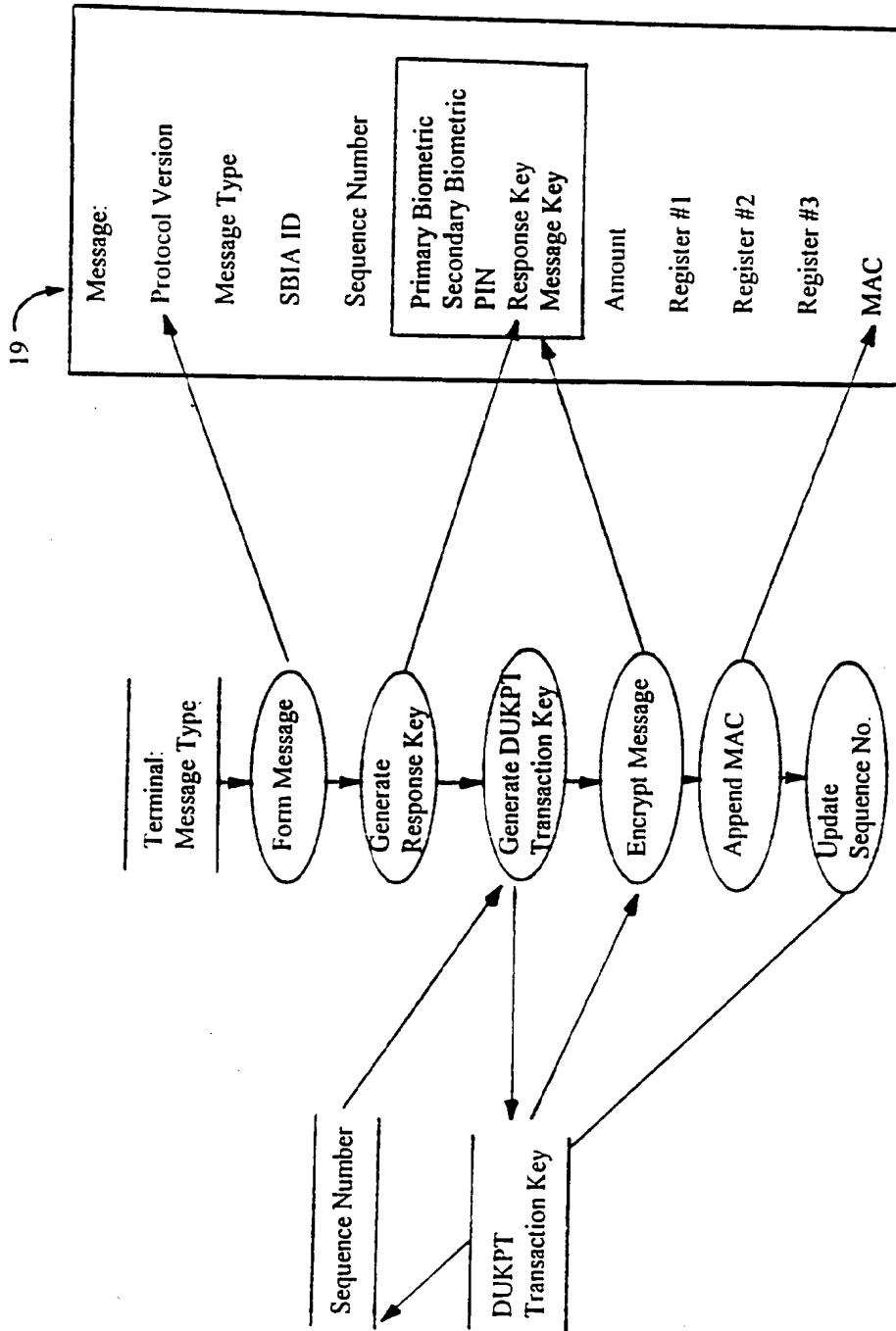


FIG. 4

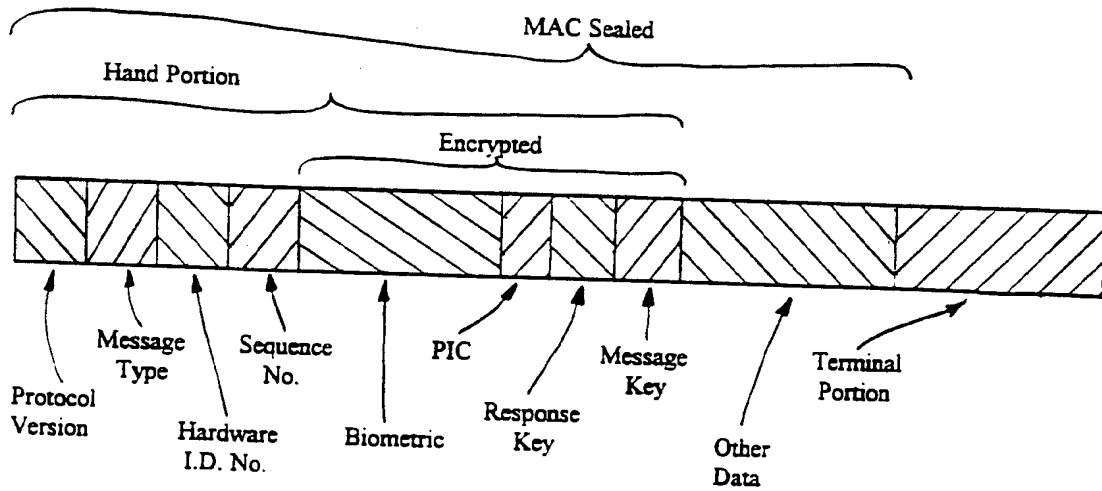


FIG. 5

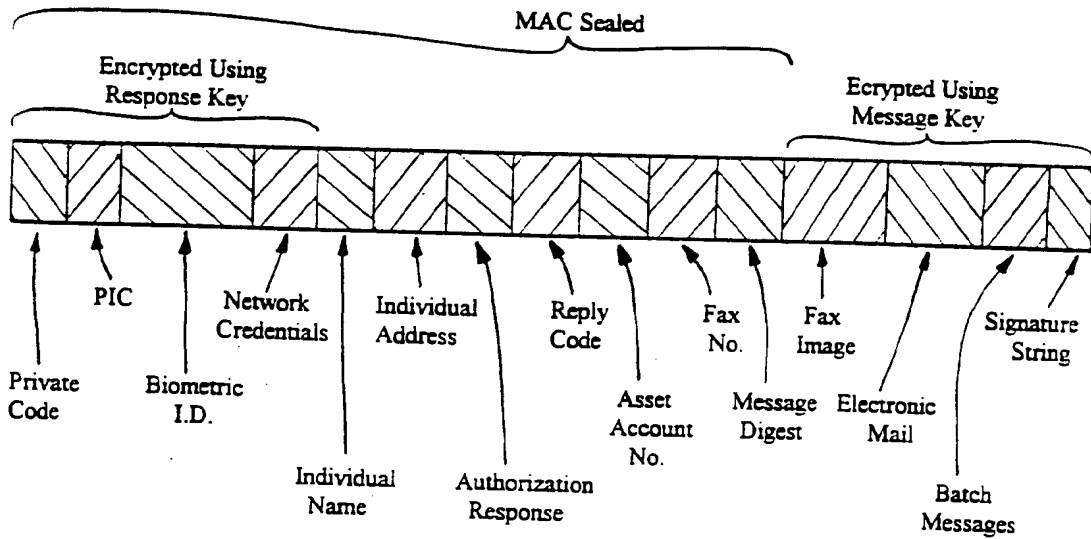


FIG. 6

6/20

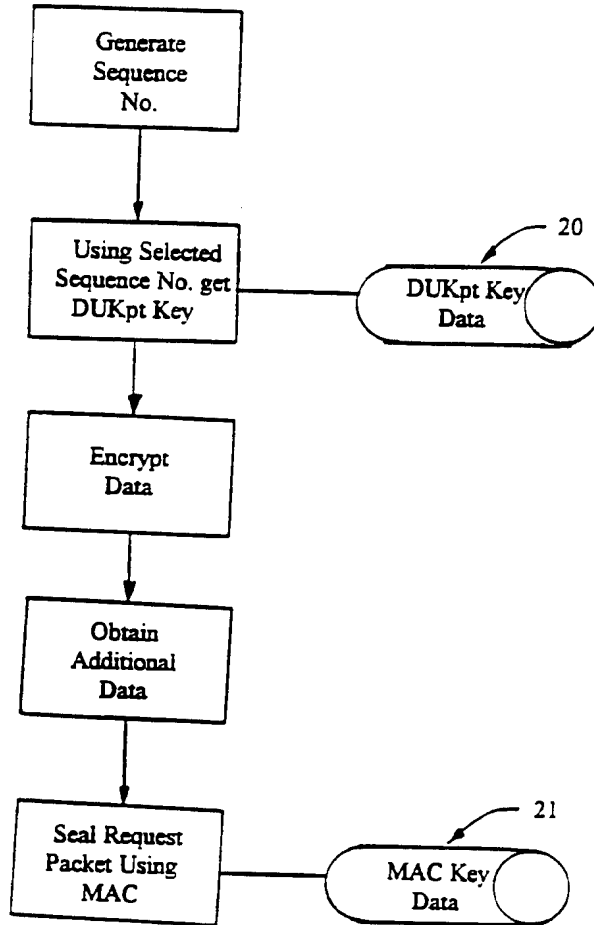


FIG. 7

7/20

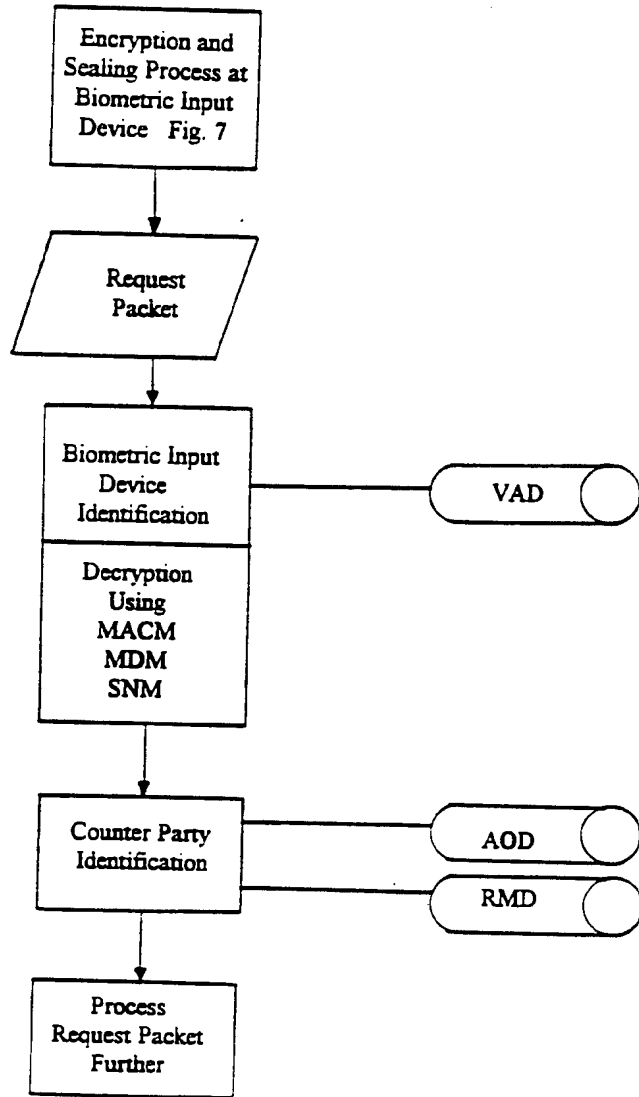


FIG. 8

8/20

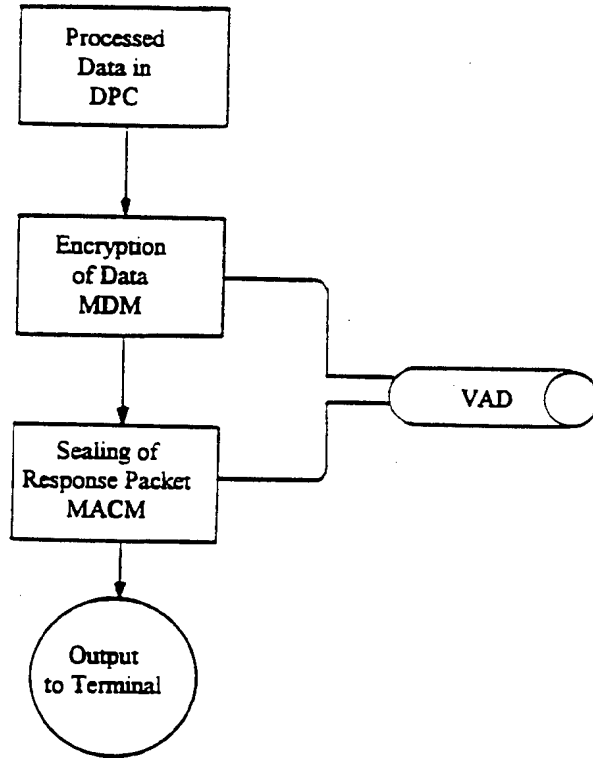


FIG. 9

9/20

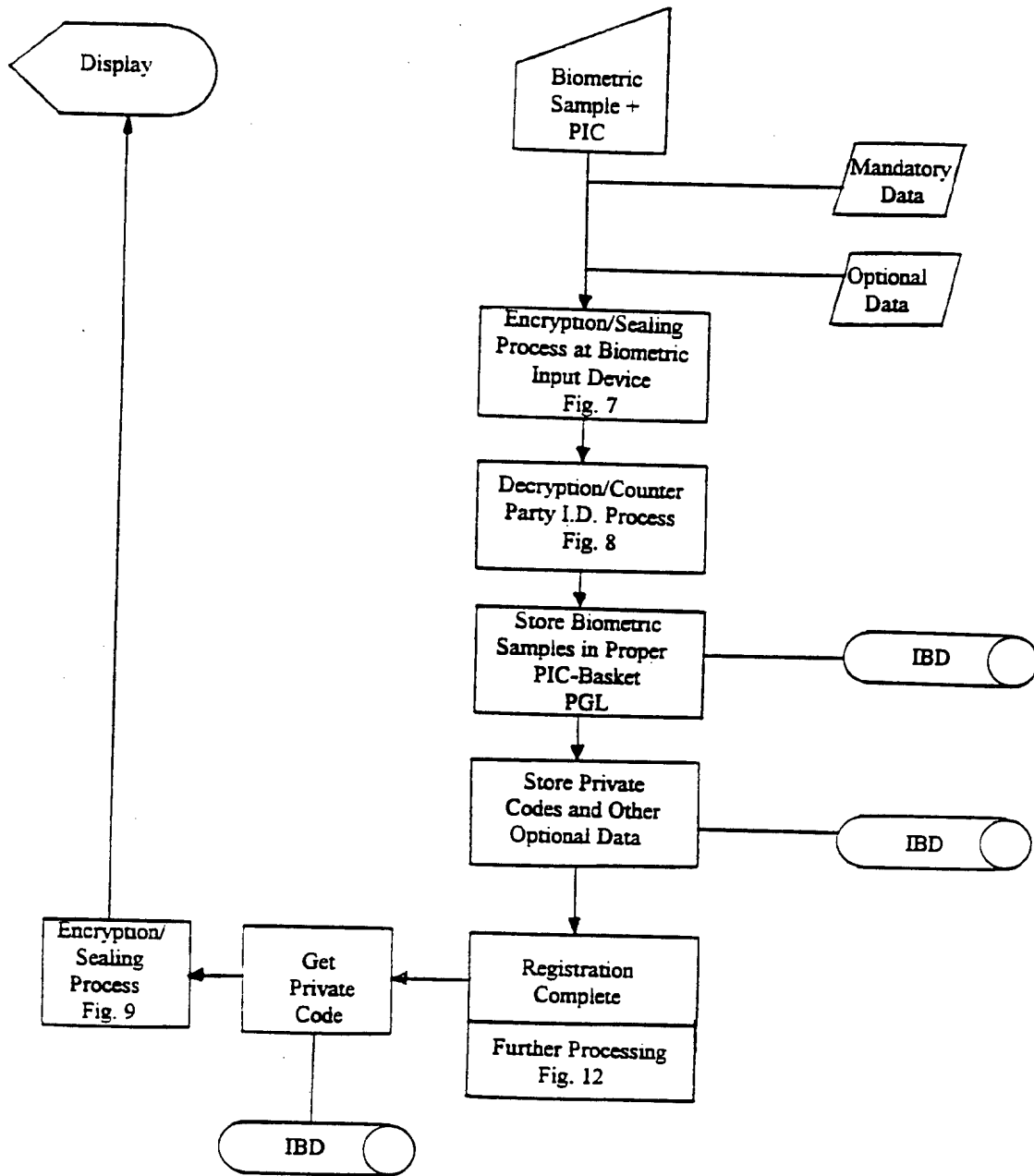


FIG. 10

10/20

PATENT

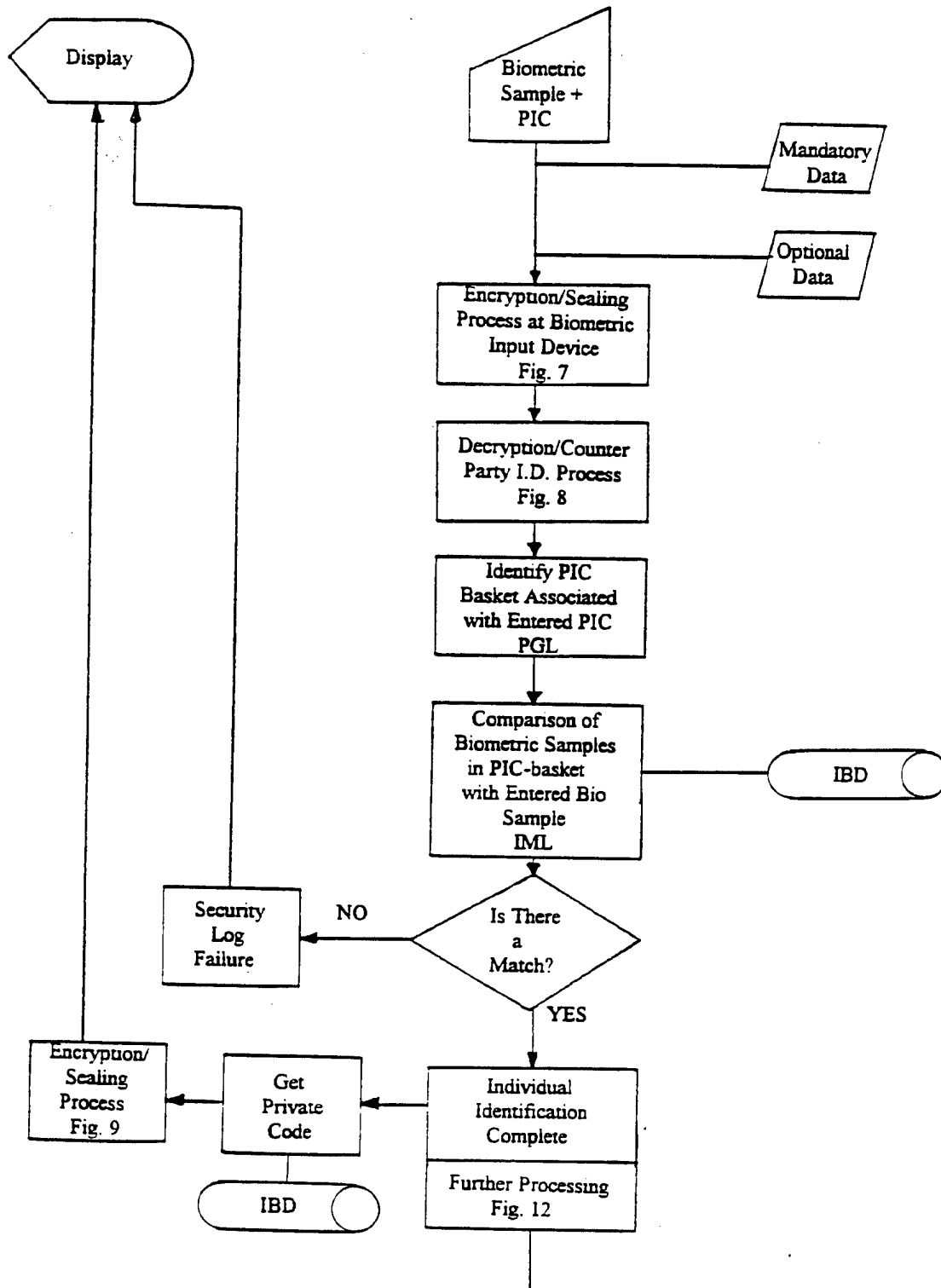


FIG. 11

11/20

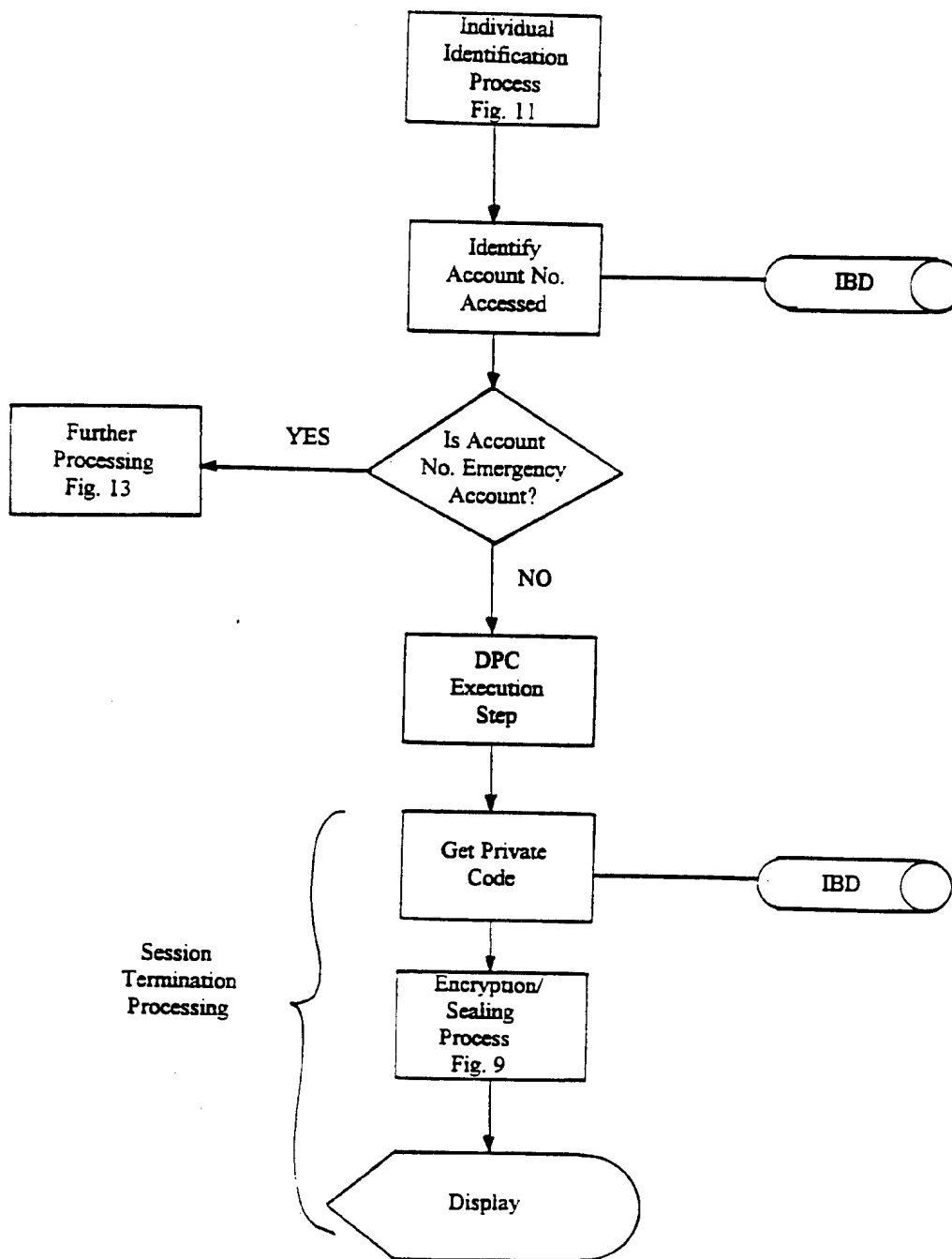


FIG. 12

12/20

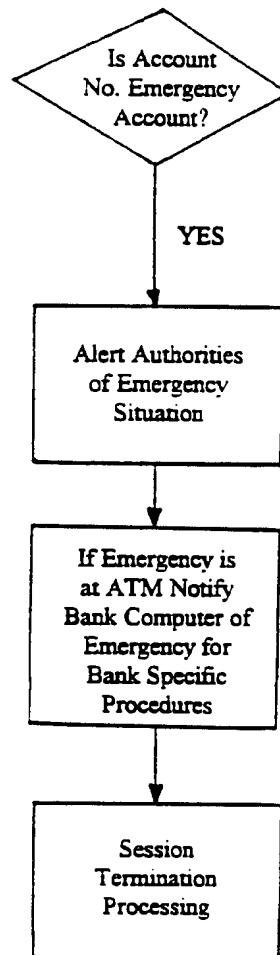


FIG. 13

13/20

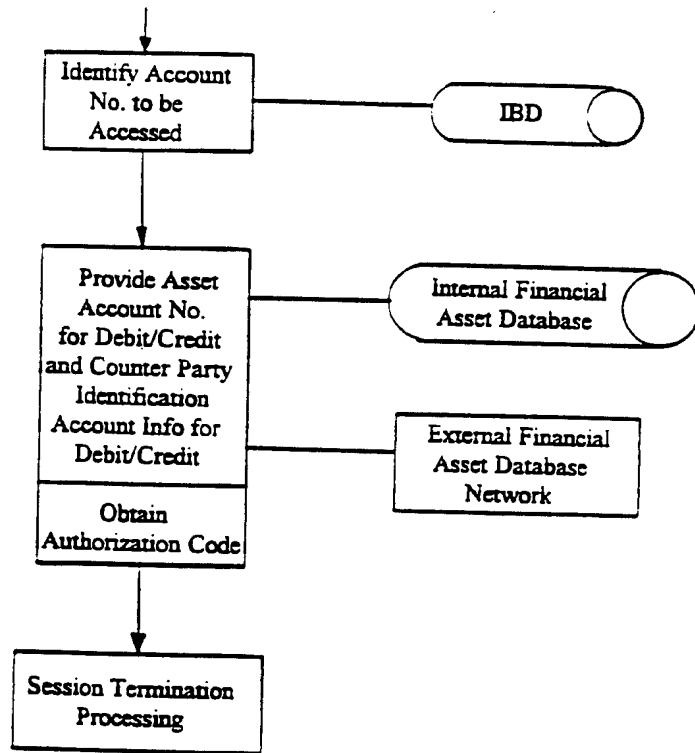


FIG. 14

14/20

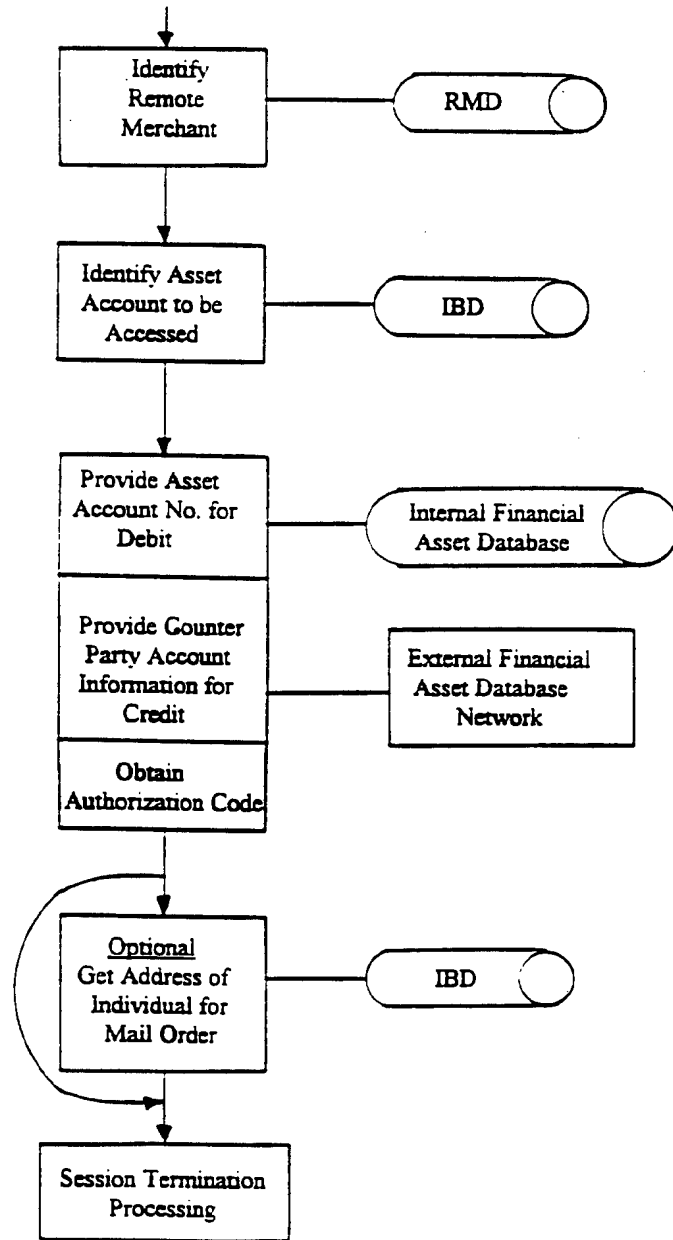


FIG. 15

15/20

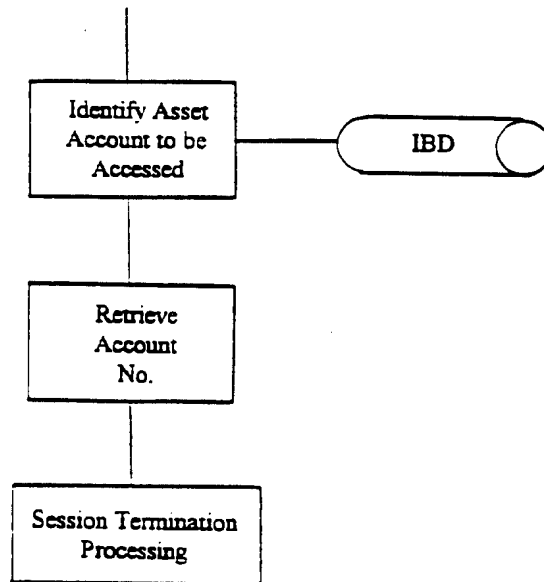


FIG. 16

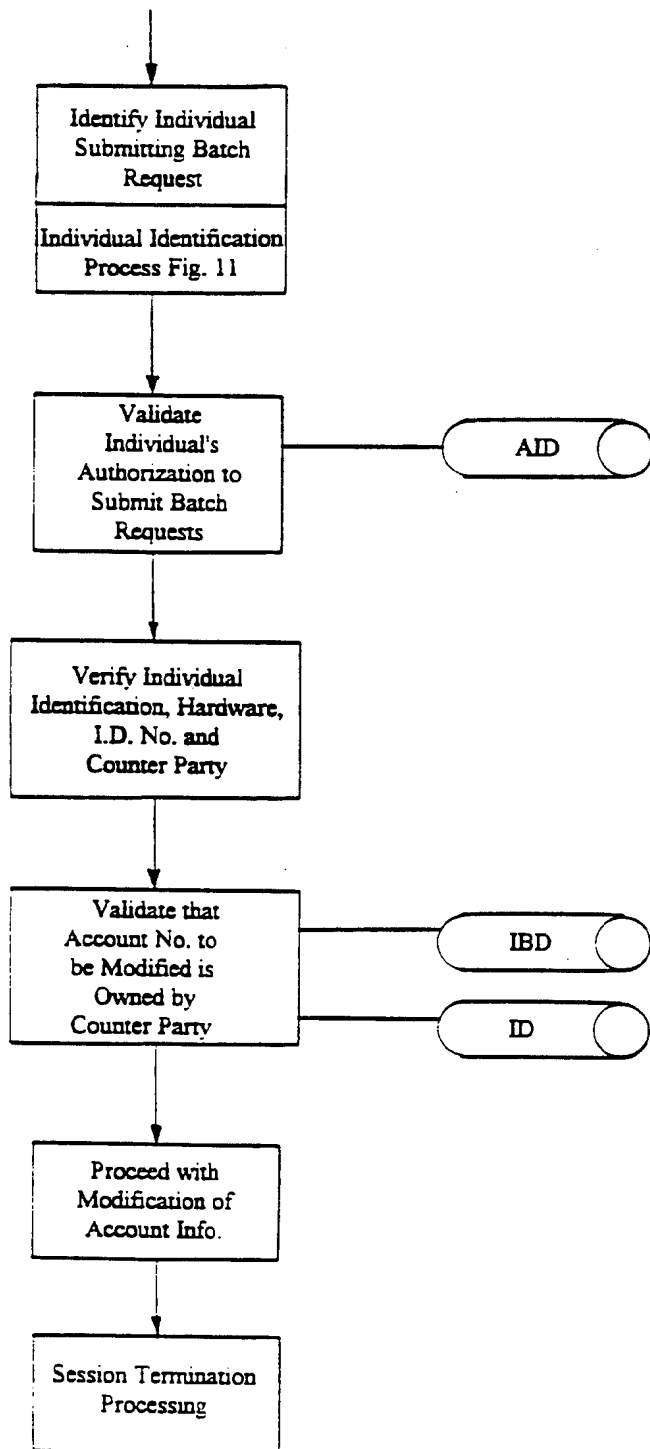


FIG. 17

17/20

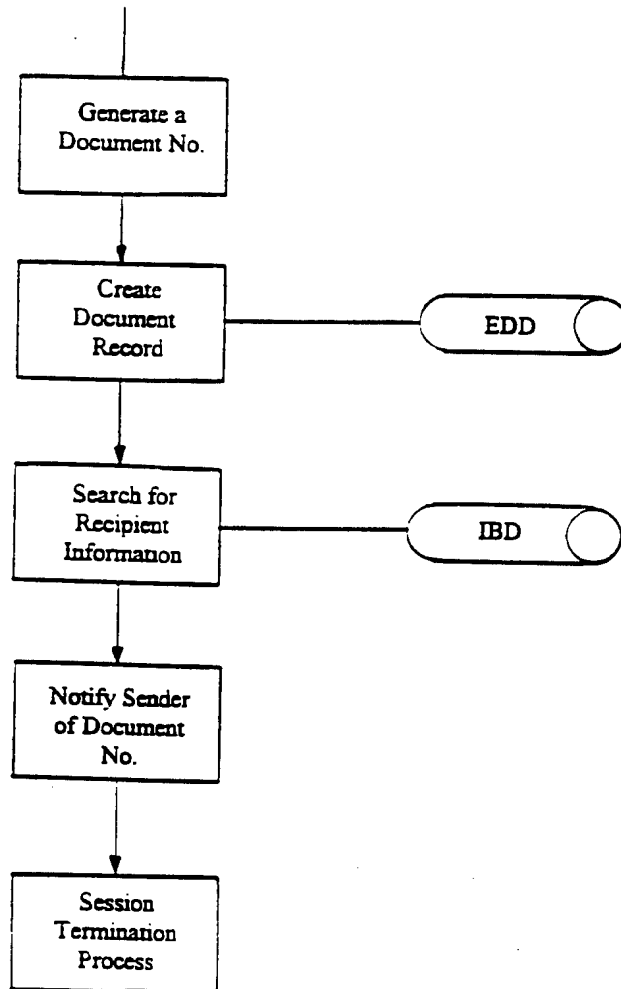


FIG. 18

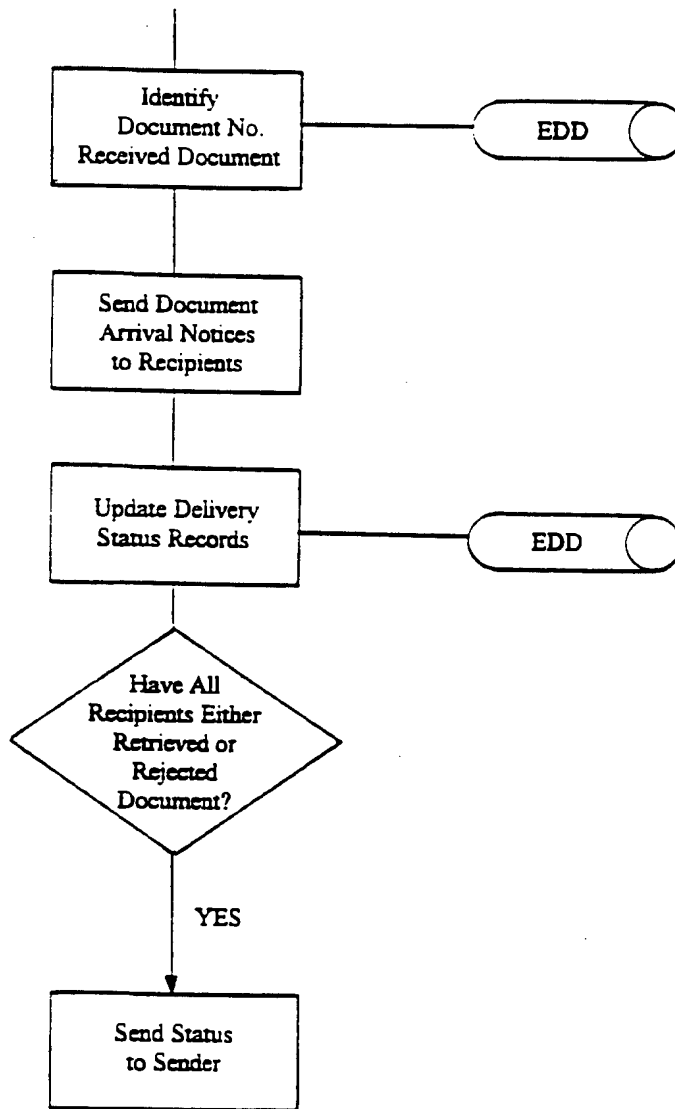


FIG. 19

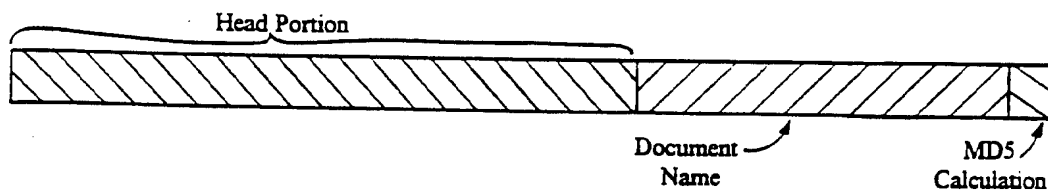


FIG. 20A

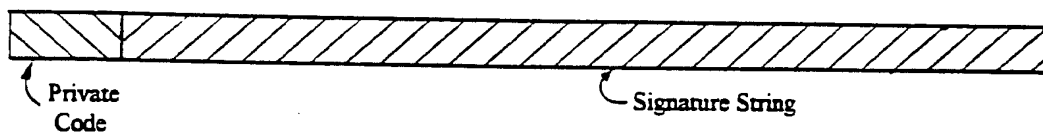


FIG. 20B

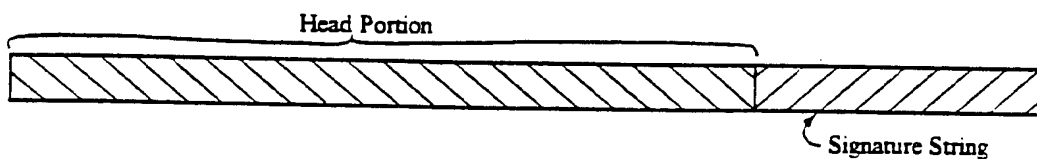


FIG. 20C

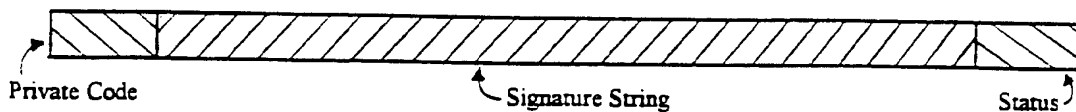


FIG. 20D

20/20

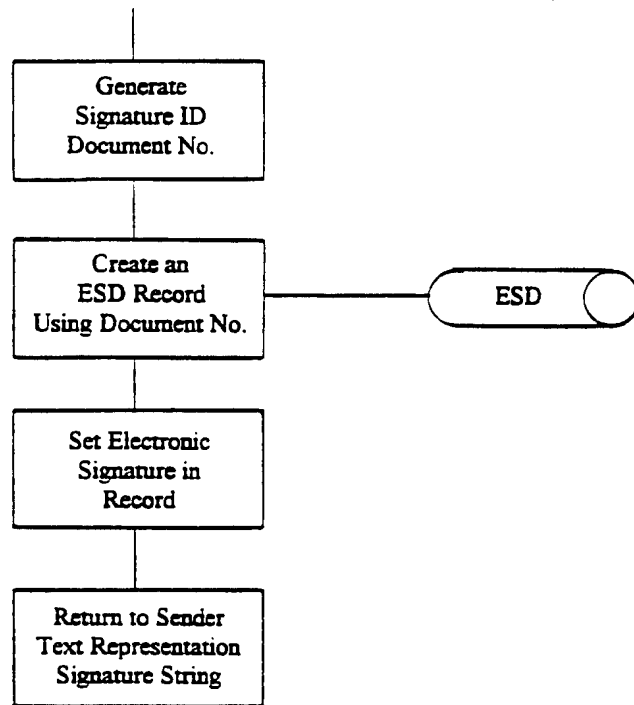


FIG. 21

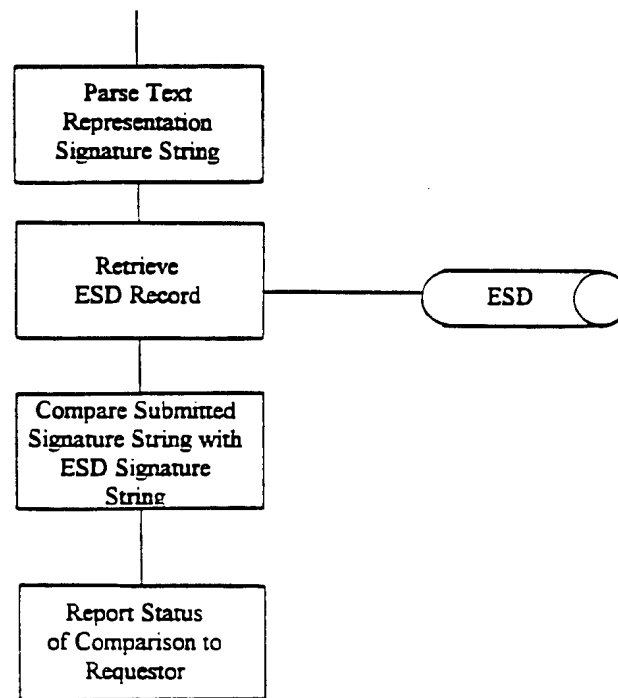


FIG. 22

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US96/07185

A. CLASSIFICATION OF SUBJECT MATTER IPC(6) :GO6K 9/00 US CL :Please See Extra Sheet. According to International Patent Classification (IPC) or to both national classification and IPC		
B. FIELDS SEARCHED Minimum documentation searched (classification system followed by classification symbols) U.S. : 902/1, 2, 3, 4, 5, 6, 22, 26, 27, 31, 32, 33; 340/825.34; 235/380; 382/115 Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched Electronic data base consulted during the international search (name of data base and, where practicable, search terms used) APS		
C. DOCUMENTS CONSIDERED TO BE RELEVANT		
Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US, A, 5,229,764 (MATCHETT ET AL) 20 July 1993, see abstract, figure 1, column 1, lines 6-59, column 8, lines 19-25.	1-87
Y	US, A, 5,191,611 (LANG) 02 March 1993, column 16, line 27.	1-87
<input type="checkbox"/> Further documents are listed in the continuation of Box C. <input type="checkbox"/> See patent family annex.		
* Special categories of cited documents:		
A document defining the general state of the art which is not considered to be part of particular relevance	*T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention	
E earlier document published on or after the international filing date	*X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone	
L document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	*Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art	
O document referring to an oral disclosure, use, exhibition or other means	*G* document member of the same patent family	
P document published prior to the international filing date but later than the priority date claimed		
Date of the actual completion of the international search	Date of mailing of the international search report	
03 JULY 1996	26 AUG 1996	
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	Authorized officer <i>Leo Boudreau</i> LEO BOUDREAU	
Facsimile No. (703) 305-3230	Telephone No. (703) 308-7595	

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US96/07185

A. CLASSIFICATION OF SUBJECT MATTER:
US CL :

902/1, 2, 3, 4, 5, 6, 22, 26, 27, 31, 32, 33; 340/825.34; 235/380; 382/115



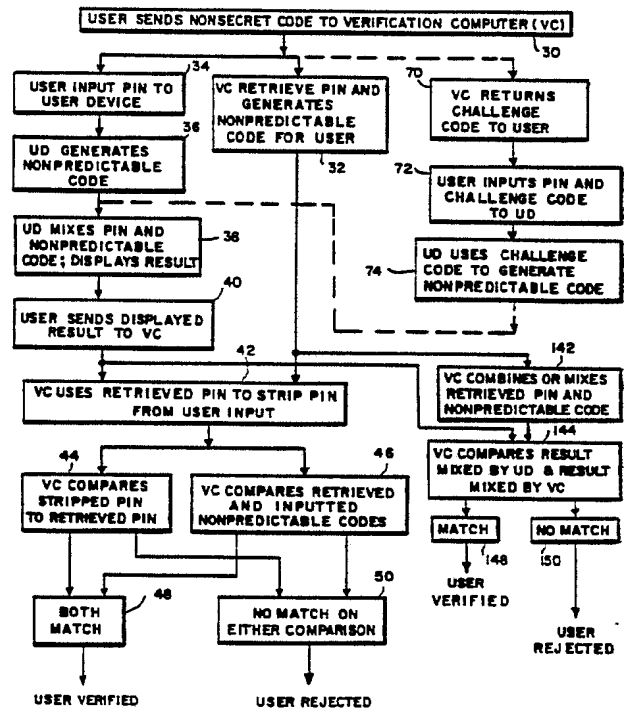
INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification ⁵ : H04K 1/00</p>	<p>A1</p>	<p>(11) International Publication Number: WO 92/07436 (43) International Publication Date: 30 April 1992 (30.04.92)</p>
<p>(21) International Application Number: PCT/US91/03034 (22) International Filing Date: 30 April 1991 (30.04.91) (30) Priority data: 597,784 19 October 1990 (19.10.90) US 670,705 18 March 1991 (18.03.91) US (71) Applicant: SECURITY DYNAMICS TECHNOLOGIES, INC. [US/US]; One Alewife Center, Cambridge, MA 02140-2312 (US). (72) Inventor: WEISS, Kenneth, P. ; 7 Park Avenue, Newton, MA 02159 (US). (74) Agent: OLIVERIO, M., Lawrence; Wolf, Greenfield & Sacks, Federal Reserve Plaza, 600 Atlantic Avenue, Boston, MA 02210 (US).</p>		<p>(81) Designated States: AT (European patent), AU, BE (European patent), CA, CH (European patent), DE (European patent), DK (European patent), ES (European patent), FR (European patent), GB (European patent), GR (European patent), IT (European patent), JP, LU (European patent), NL (European patent), SE (European patent). Published <i>With international search report.</i></p>

(54) Title: METHOD AND APPARATUS FOR PERSONAL IDENTIFICATION

(57) Abstract

A method and apparatus for providing improved security for a personal identification number (PIN) in a personal identification and verification system of the type wherein a time dependent nonpredictable code is generated at a device in the possession of the individual (36), which code is unique to the individual and this code is communicated to, and compared with a nonpredictable code generated at a central verification computer (46). In this system, the PIN is mixed with the nonpredictable code before transmission of these values to the central verification computer (38). A nonsecret code (30) is previously transmitted to the central verification computer and is used by the verification computer to retrieve the PIN and independently generate the time dependent appropriate nonpredictable code for the user (74). These retrieved PIN and generated code values are used by the verification computer either (a) to strip the PIN from the transmitted nonpredictable code (42) and the stripped PIN and remaining nonpredictable code are compared with the corresponding retrieved values in order to determine verification (44, 46); or (b) to be mixed and then compared with the mixed PIN and code which is transmitted to the verification computer (144).



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	ES	Spain	MG	Madagascar
AU	Australia	FI	Finland	ML	Mali
BB	Barbados	FR	France	MN	Mongolia
BE	Belgium	GA	Gabon	MR	Mauritania
BF	Burkina Faso	GB	United Kingdom	MW	Malawi
BG	Bulgaria	GN	Guinea	NL	Netherlands
BJ	Benin	GR	Greece	NO	Norway
BR	Brazil	HU	Hungary	PL	Poland
CA	Canada	IT	Italy	RO	Romania
CF	Central African Republic	JP	Japan	SD	Sudan
CG	Congo	KP	Democratic People's Republic of Korea	SE	Sweden
CH	Switzerland	KR	Republic of Korea	SN	Senegal
CI	Côte d'Ivoire	LI	Liechtenstein	SU⁺	Soviet Union
CM	Cameroon	LK	Sri Lanka	TD	Chad
CS	Czechoslovakia	LU	Luxembourg	TC	Togo
DE⁺	Germany	MC	Monaco	US	United States of America
DK	Denmark				

+ Any designation of "SU" has effect in the Russian Federation. It is not yet known whether any such designation has effect in other States of the former Soviet Union.

- 1 -

METHOD AND APPARATUS FOR PERSONAL IDENTIFICATIONCross Reference to Other Applications

5 This application is a continuation-in-part of
application serial no. 07/341,932 filed April 21,
1989, which is a continuation-in-part of application
10 serial no. 802,579 filed November 27, 1985, issued
December 5, 1989 as U.S. Patent No. 4,885,778,
which application is itself a continuation-in-part
of application serial no. 676,626 filed November 30,
1984, now U.S. Patent No. 4,720,860, issued January
19, 1988. The disclosures and specifications of all
of the foregoing applications/patents are incor-
porated herein by reference as if fully set forth.

- 2 -

Field of the Invention

This invention relates to methods and apparatus for identifying an individual and more particularly to methods and apparatus for providing improved security for a personal identification number (PIN) utilized in conjunction with such an identification system.

Background of the Invention

Personal identification systems may be based on something someone has, such as a card or badge, something that someone knows, such as a PIN, or some characteristic of the individual, such as his fingerprints or speech pattern. Security for such systems is enhanced by utilizing two or more of the above in performing the identification.

For example, parent Patent No. 4,720,860, discloses a personal identification system wherein the individual has a card or other small, portable device which contains a microprocessor programmed to utilize a secret algorithm to generate a nonpredictable number from a stored value unique to the individual and a time varying value provided for example by a clock. The nonpredictable value is preferably displayed on the device. The individual then enters his secret PIN into a central verification system, either directly or over a telephone line, causing the central system to access

- 3 -

stored information corresponding to the individual and to utilize at least some of this information to generate a nonpredictable value at the central computer utilizing the same algorithm as at the individual's microprocessor. At the same time this is being done, the individual is entering the number appearing at that period of time on the display of his device. The two values will match, signifying identification of the individual, only if the individual has entered the correct PIN and if the individual has the proper device so that the nonpredictable code displayed corresponds to that being generated at the central verification computer.

In other systems, such as those shown in U.S. Patent No. 4,599,489 issued July 8, 1986, the PIN may either be stored in the user's device, or may be entered by the user. If the PIN is stored in the device, it is read from the device by a suitable reader and causes the central verification computer to generate a unique challenge code to the individual. This challenge code may either be entered by the individual into his machine, or may be automatically sensed by the machine, and is operated on by the user's device to generate a unique nonpredictable code which is then entered into the central computer to effect verification.

One potential difficulty with either of the systems indicated above is that an unauthorized

- 4 -

individual may be able to obtain access to the user's PIN by electronic eavesdropping, reducing the security provided by the system. If, for example, the PIN is transmitted over public lines, such as telephone lines, from the user to the central verification computer, it may be possible to tap these lines and intercept the PIN as it is being transmitted. If the PIN is stored in the device, someone obtaining the device surreptitiously may, through sophisticated means, be able to determine the PIN stored in the device and thus defeat the security of the system. Furthermore, any storing of a PIN or password in the portable device for comparison defeats the purpose of an independent identification factor and reduces security to a "thing" possessed.

A need therefore exists for an improved means of communicating a PIN or other user identification code to a central verification system such that someone tapping the line over which the code is being sent will be unable to determine the secret identification number and someone obtaining possession of the user device will also not be able to obtain access to the user's secret identification number from the device.

- 5 -

Summary of the Invention

In accordance with the above, this invention provides a method for personal identification and apparatus for the practice thereof wherein a device
5 in the possession of the individual is utilized to generate a unique, time varying, nonpredictable code; the nonpredictable code generated at a given time is mixed with a secret PIN for the individual; the mixed output is communicated to a central
10 verification computer; and the verification computer typically strips the PIN from the communicated value and utilizes the stripped PIN and remaining nonpredictable code to perform a verification operation. Alternatively and equivalently, the
15 mixed output which is communicated to the verification computer may be verified in the verification computer without stripping of the PIN. Preferably, before the mixed value is communicated to the verification computer, a nonsecret
20 identifying code for the individual is communicated to the verification computer; the verification computer utilizes the nonsecret identifying code to obtain the PIN and appropriate nonpredictable code for the individual; and the verification operation
25 includes the PIN and appropriate nonpredictable code obtained during the obtaining step being compared with the stripped PIN and remaining nonpredictable code. Alternatively the PIN may not be stripped

- 6 -

from the mixed value, the verification computer may utilize the nonsecret identifying code to retrieve or obtain the PIN and appropriate nonpredictable code, combine the retrieved PIN and appropriate nonpredictable code, and perform a verification operation between the mixed value communicated to the verification computer and the combination of the retrieved PIN and appropriate nonpredictable code. The verification computer may also generate a unique challenge value in response to the nonsecret identifying code which challenge code is communicated to the device in possession of the individual. For one embodiment, the challenge code is communicated to the individual and the individual inputs the challenge value and the PIN to his device, the device includes means responsive to the challenge value for generating the nonpredictable code. During the mixing step, the device may receive the PIN and the nonpredictable code and generate an output which is a predetermined function of the inputs. The predetermined function may, for example, be a sum of the inputs, for example the sum of the inputs without carry.

The foregoing and other objects, features and advantages of the invention will be apparent from the following more particular description of preferred embodiments of the invention as illustrated in the accompanying drawings.

- 7 -

In the Drawings

Fig. 1 is a semi-block schematic diagram of the verification system of a first embodiment of the invention.

5 Fig. 2 is a block schematic diagram of a second embodiment of the invention.

Fig. 3 is a block flow diagram illustrating the operation of the first embodiment of the invention and alternative steps for the second embodiment of the invention.

10

Detailed Description

Fig. 1 shows illustrative structure for a personal identification system of a first embodiment of the invention. In this figure, a user verification device 10 is provided which is of the type described in the parent applications. The device is preferably of the general size and shape of a standard credit card, although its thickness dimension may be slightly greater than that of such cards. The device 10 has a clock which generates a time-dependent digital output to a microprocessor which is programmed with a unique algorithm to operate on the time-dependent clock input and on a stored static value unique to a given user to generate a multi-bit nonpredictable code. A plurality of input areas 12 are provided on the face of device 10. These areas are preferably each

15

20

25

- 8 -

indicative of a numerical digit, for example the digits 1 - 0 as shown in Fig. 1, and may be pressure-sensitive pads or otherwise adapted to generate an electrical output indicative of the area when the area is touched by the user. Spacing may be provided between the individual areas 12 to assure distinctive outputs. As will be described in greater detail hereinafter, the user may input his unique PIN on areas 12 which are mixed in the processor in device 10 with the nonpredictable code generated therein in response to the time-dependent and static inputs to generate a multi-bit nonpredictable code which is displayed on area 14 of device 10. Area 14 may be a liquid crystal display or other suitable display device for producing numeric or alpha-numeric characters. Each area of display 14 is adapted to display a different digit of the nonpredictable code.

The user initially transmits a nonsecret identifying code to verification computer 16 by keying this number into a telephone 18 at his location. This number is transmitted over telephone lines 20 to telephone 22 at the verification station and through a modem 24 at this station to the verification computer. The user may then use the telephone 18 to key in and transmit the nonpredictable code being displayed at that time on display 14.

- 9 -

Fig. 3 is a flow diagram illustrating in greater detail the operation of the system of Fig. 1 to perform a verification operation. Referring to Fig. 3, the first step in the operation, step 30, is for the user to send his nonsecret code to verification computer (VC) 16. As previously indicated, this is accomplished by the user keying his nonsecret identification number into telephone 18 for transmission through telephone line 20, telephone 22 and modem 24 to the verification computer.

In response to the user input of his nonsecret code, the verification computer retrieves the user's PIN and generates the nonpredictable code for the user, using the same algorithm and stored static value as user device 10, and using a time-related value from a clock device at the verification computer, which is maintained in synchronism with the clock at the user device in a manner discussed in the parent application (step 32). At the same time that the verification computer is retrieving the PIN and nonpredictable code for the user, the user is inputting his PIN into his device 10 using key pads or areas 12 (step 34). While the user is inputting his pin, the user device is continuously generating nonpredictable code values at its internal processor in response to the clock value and the stored static value using the unique algorithm at the user device processor (step 36).

- 10 -

The next step in the operation, step 38, is for the generated nonpredictable code and the inputted pin to be mixed by the processor in device 10 to generate a new nonpredictable code which is
5 displayed on display 14. The mixing operation may be a simple addition of the two values without carry, or with carry, (a constant added to a pseudo random number produces a pseudo random number) or may involve a more sophisticated mixing algorithm.

10 During step 40, the user transmits the displayed value by use of telephone 18 through telephone line 20, telephone 22, and modem 24 to verification computer 16.

15 During the next step in the operation, step 42, the verification computer uses the PIN for the user which was retrieved during step 32 to strip the PIN from the inputted nonpredictable code, the result being a PIN value and a nonpredictable code value. During step 44 the stripped PIN is compared with the
20 PIN retrieved during step 32 and during step 46 the nonpredictable code remaining after the inputted value has the PIN stripped therefrom is compared with the retrieved nonpredictable code. If matches are obtained during both steps 44 and 46 (step 48)
25 the verification computer signifies verification. If a match is not found during either step 44 or step 46 (step 50) then the user is rejected.

- 11 -

Alternatively to steps 42, 44, 46, 48 and 50,
the PIN and nonpredictable code which are retrieved
in step 32 may be combined or mixed by the
verification computer during step 142 according to
5 the same mixing operation which was carried out by
the processor or user device 10 in step 38, e.g. by
a simple addition of the two values without carry,
with carry, or according to some other more
sophisticated algorithm. During alternative step
10 144 the separate results of the mixing operations
carried out by the user device 10 and the
verification computer 16 are compared. If a match
is obtained, step 148, the user is verified. If a
match is not found, step 150, the user is rejected.

15 A procedure is thus provided wherein user
verification may be obtained using the simple and
inexpensive procedure disclosed in the parent
applications while still providing a high level of
security for the user PIN. This security is
20 achieved since the user PIN is never available on an
open line which could be tapped except in the form
of a word which is a mixture of the PIN with a
nonpredictable code and which is virtually
impossible to decipher.

25 Fig. 2 illustrates an alternative configuration
in which the teachings of this invention may be
utilized. In Fig. 2, the user device 10 is of the
same type shown in Fig. 1. However, for this

- 12 -

embodiment of the invention, the user device is adapted to be used in proximity to the verification station rather than from a remote location over telephone lines. For this embodiment of the invention, the verification station 60 includes a computer 62, a display 64, such as for example a CRT display, and an input device 66 which may, for example, be a standard computer input keyboard. Referring again to Fig. 3, the operation with this embodiment of the invention starts with step 30, during which the user sends a nonsecret code to the verification computer 62 by, for example, keying this code into input device 66. In response to receiving the nonsecret code, computer 60 retrieves the PIN and generates the nonpredictable code for the user (step 32) and also retrieves a challenge code for the user which is displayed on display 64 (step 70). The user inputs his PIN and the challenge code in an order established for the system to user device 10 using input pads 12 (step 72). During step 74, the processor in device 10 uses the inputted challenge code and the time inputted from its clock to generate a nonpredictable code which, during step 38, is mixed with the inputted pin and the results are displayed on display 14 of device 10. From this point on, the operation for this embodiment of the invention is the same as that previously described with respect to the embodiment of Fig. 1.

- 13 -

Thus, with this embodiment of the invention, as with the prior embodiment of the invention, the pin in uncoded form is never transmitted in a manner such that it could be observed and is not resident in the user's device where it might, using sophisticated technology, be retrieved.

As an alternative to the embodiment shown in Fig. 2, the nonsecret code may be recorded in machine-readable form on device 10 and input device 66 might include a card reader which the card is inserted into to permit the nonsecret code to be read into computer 62.

While the invention has been shown and described above with reference to preferred embodiments, the foregoing and other changes in form and detail may be made therein by one skilled in the art without departing from the spirit and scope of the invention.

What is claimed is:

- 14 -

CLAIMS

1. In a personal identification system of the type wherein a user is provided with a device generating a unique, time-varying, nonpredictable code, with a nonsecret identifying code and with a secret PIN, the nonpredictable code at a given instant and the PIN being provided to a central verification computer to effect verification; apparatus for providing improved security for the PIN comprising:

means for mixing the nonpredictable code generated by the device at a given time with the PIN according to a predetermined algorithm to generate a combined coded value;

means for separately communicating the nonsecret identifying code and the combined coded value to the central verification computer; and

wherein the central verification computer includes means for utilizing the nonsecret identifying code to retrieve the PIN and generate an appropriate, unique, time varying nonpredictable code for the individual, and at least one of:

(a) a means for utilizing the retrieved PIN, appropriate nonpredictable code and the combined coded value in performing a verification operation; or

- 15 -

(b) a means for stripping the PIN from the combined coded value received from the means for communicating, the nonpredictable code remaining after stripping of the PIN and means for utilizing the retrieved PIN, and appropriate nonpredictable code for performing a verification operation.

2. Apparatus as claimed in claim 1 including means operative prior to the communicating of the value from the mixing means for communicating the nonsecret identifying code to said verification computer.

3. Apparatus as claimed in claim 2 wherein said verification computer includes means for utilizing the communicated nonsecret identifying code to retrieve the PIN and a unique challenge value for the individual; and means for communicating the challenge value to the device.

4. Apparatus as claimed in claim 3 wherein said challenge value communicating means includes means for communicating the challenge value to the individual; and wherein the device includes means for permitting the individual to input the challenge value and his PIN to the device.

- 16 -

5. Apparatus as claimed in claim 4 wherein said device includes means responsive to the challenge value for generating the nonpredictable code; and

5 wherein said mixing means includes means, included as part of the device, for receiving the inputted PIN and the generated nonpredictable value and for generating an output which is a predetermined function of the input.

10 6. Apparatus as claimed in claim 5 wherein said mixing means adds the PIN to the nonpredictable code.

7. Apparatus as claimed in claim 1 wherein said device includes means for permitting the individual to input his PIN to the device; and

15 wherein said means for mixing is included as part of said device and is adapted to receive the PIN inputted by the individual and the nonpredictable code and to generate an output which

20 is a predetermined function of the input.

8. Apparatus as claimed in claim 7 wherein said mixing means adds the PIN to the nonpredictable code.

- 17 -

9. Apparatus as claimed in claim 1 wherein
said verification computer includes a means for
mixing the retrieved PIN and appropriate
nonpredictable code generated by the verification
computer at a given time according to the
predetermined algorithm to generate a second
combined coded value.

5

10. Apparatus as claimed in claim 9 wherein the
verification operation comprises comparing the
combined coded value with the second combined coded
value.

10

11. Apparatus as claimed in claim 1 wherein the
means for performing a verification operation
includes means for comparing the PIN and
nonpredictable code obtained in response to the
nonsecret identifying code with the stripped PIN and
remaining nonpredictable code.

15

12. A method for identifying an individual
comprising the steps of:

20

utilizing a device in the possession of the
individual to generate a unique time-varying,
nonpredictable code;

mixing the nonpredictable code generated at
a given time with a secret PIN for the individual to
generate a combined code; and

25

- 18 -

communicating a nonsecret identifying code for the individual and the combined code to a central verification computer;

5 the verification computer utilizing the nonsecret identifying code to retrieve the PIN and generate an appropriate, unique, time-varying nonpredictable code for the individual, and at least one of:

10 (a) utilizing the retrieved PIN, appropriate nonpredictable code, and the combined code to perform a verification operation; or

15 (b) stripping the PIN from the communicated combined code and utilizing the retrieved PIN and nonpredictable code, the stripped PIN and the remaining nonpredictable code to perform a verification operation.

13. A method as claimed in claim 12 wherein the verification computer also generates a unique challenge value in response to the nonsecret identifying code; and
20 including the step of communicating the challenge value to the device in possession of the individual.

14. A method as claimed in claim 13 wherein the challenge value is communicated to the individual;
25 and

including the step of the individual inputting the challenge value and his PIN to the device.

5 15. A method as claimed in claim 14 wherein the device includes means responsive to the challenge value for generating the nonpredictable code; and
wherein the mixing step includes the device receiving the PIN and the nonpredictable code and generating an output which is a predetermined
10 function of the inputs.

16. A method as claimed in claim 15 wherein said predetermined function is a sum of said inputs.

15 17. A method as claimed in claim 15 including the step of the individual inputting his PIN to the device; and
wherein the mixing step includes the device receiving the PIN inputted by the individual and the nonpredictable code and generating an output which is a predetermined function of the inputs.

20 18. A method as claimed in claim 17 wherein said predetermined function is a sum of said input.

19. A method as claimed in claim 12 wherein the verification computer utilizes the retrieved PIN and

- 20 -

appropriate nonpredictable code by combining them to obtain a second combined code.

20. A method as claimed in claim 19 wherein the verification operation comprises comparing the
5 combined code and the second combined code.

21. A method as claimed in claim 12 wherein the verification operation includes comparing the
retrieved PIN and the nonpredictable code generated
by the verification computer with the stripped PIN
10 and the remaining nonpredictable code.

1/2

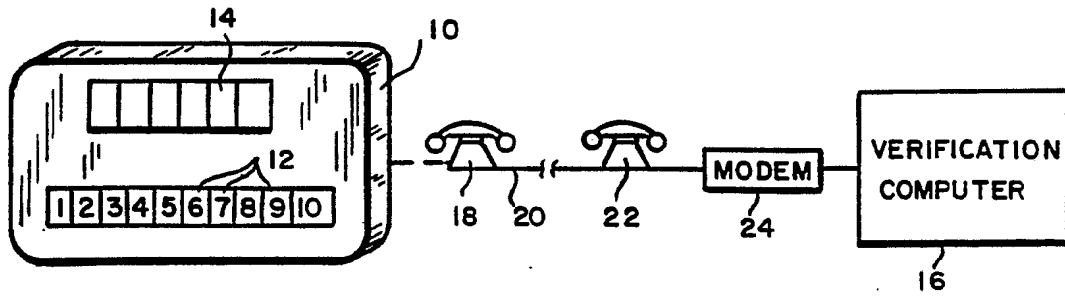


FIG. 1

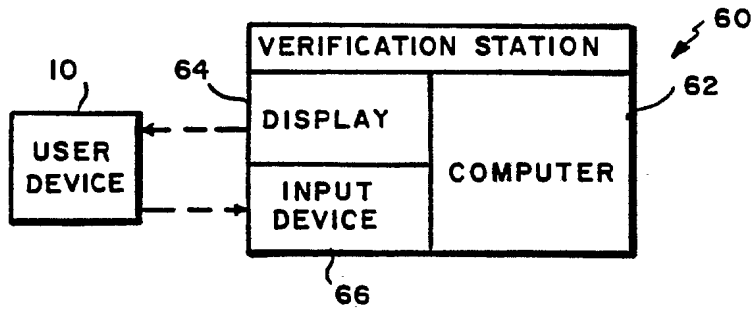


FIG. 2

2/2

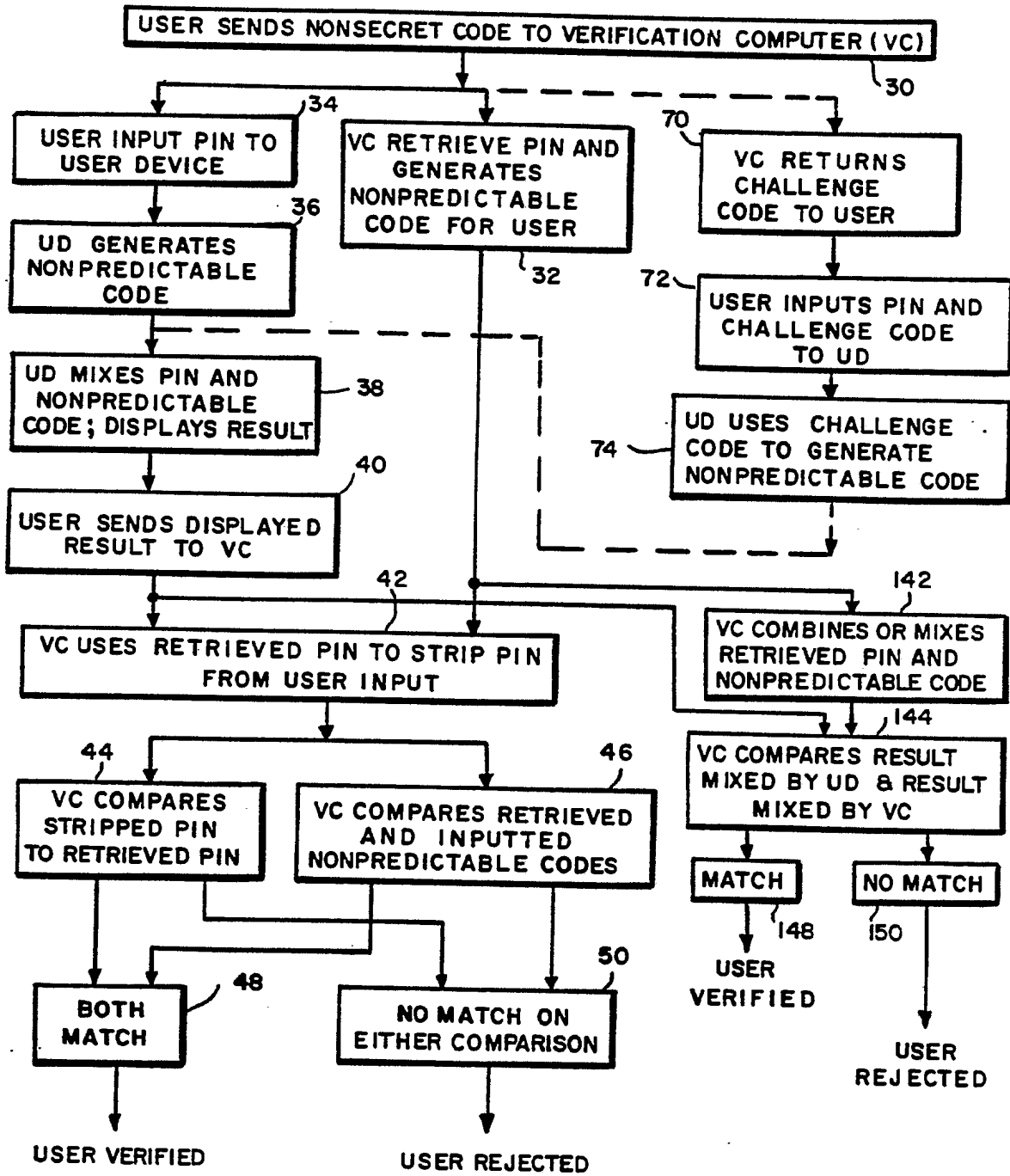


FIG. 3

INTERNATIONAL SEARCH REPORT

International Application No. **PCT/US91/03034**

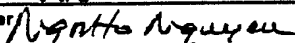
I. CLASSIFICATION OF SUBJECT MATTER (if several classification symbols apply, indicate all) ⁶		
According to International Patent Classification (IPC) or to both National Classification and IPC		
IPC(5) H04K 1/00 US 380/23,25		
II. FIELDS SEARCHED		
Minimum Documentation Searched ⁷		
Classification System	Classification Symbols	
US	380/23,24,25,28,48	
Documentation Searched other than Minimum Documentation to the Extent that such Documents are Included in the Fields Searched ⁸		
III. DOCUMENTS CONSIDERED TO BE RELEVANT ⁹		
Category ¹⁰	Citation of Document, ¹¹ with indication, where appropriate, of the relevant passages ¹²	Relevant to Claim No. ¹³
X	US,A 4,720,860 (WEISS) 19 January 1988	1-21
A	US,A 4,890,323 (BEKER ET AL) 26 December 1989	1-21
A	US,A 4,885,778 (WEISS) 05 December 1989	1-21
A	US,A 4,856,062 (WEISS) 08 August 1989	1-21
A	US,A 4,819,267 (CARGILE ET AL) 04 April 1989	1-21
A	US,A 4,802,216 (IRWIN ET AL) 31 January 1989	1-21
A	US,A 4,731,841 (ROSEN ET AL) 15 March 1988	1-21
A	US,A 4,599,489 (CARGILE) 08 July 1986	1-21
A	US,A 4,578,530 (ZEIDLER) 25 March 1986	1-21
A	US,A 4,509,093 (STELLBERGER) 02 April 1985	1-21
<p>¹⁰ Special categories of cited documents:</p> <p>"A" document defining the general state of the art which is not considered to be of particular relevance</p> <p>"E" earlier document but published on or after the international filing date</p> <p>"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>"O" document referring to an oral disclosure, use, exhibition or other means</p> <p>"P" document published prior to the international filing date but later than the priority date claimed</p> <p>"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step</p> <p>"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.</p> <p>"&" document member of the same patent family</p>		
IV. CERTIFICATION		
Date of the Actual Completion of the International Search	Date of Mailing of this International Search Report	
21 August 1991	27 SEP 1991	
International Searching Authority	Signature of Authorized Officer	
ISA/US	 NGUYEN NGOC-HO INTERNATIONAL DIVISION	
		David Cain

FIG. 1
(PRIOR ART)

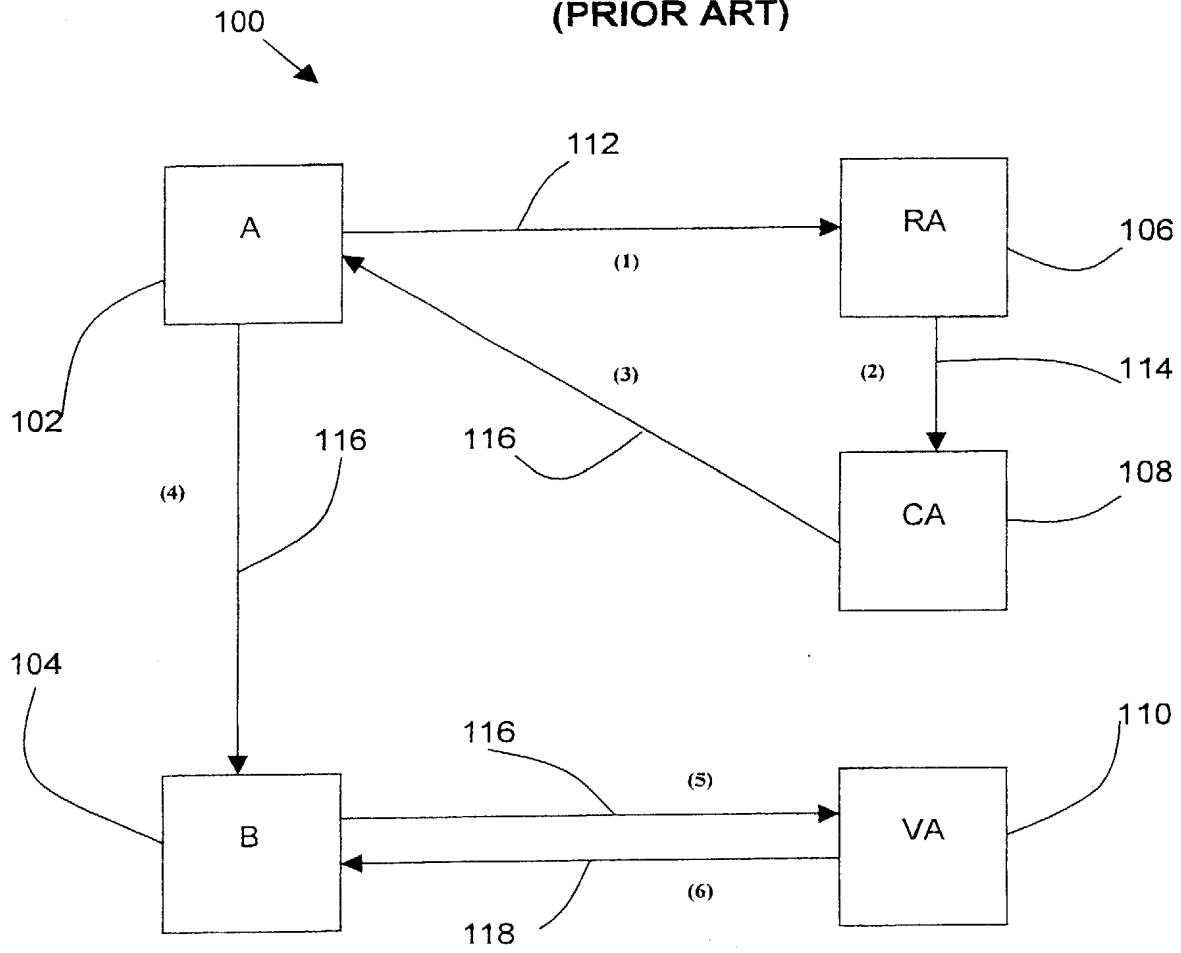


FIG. 2

(PRIOR ART)

200 →

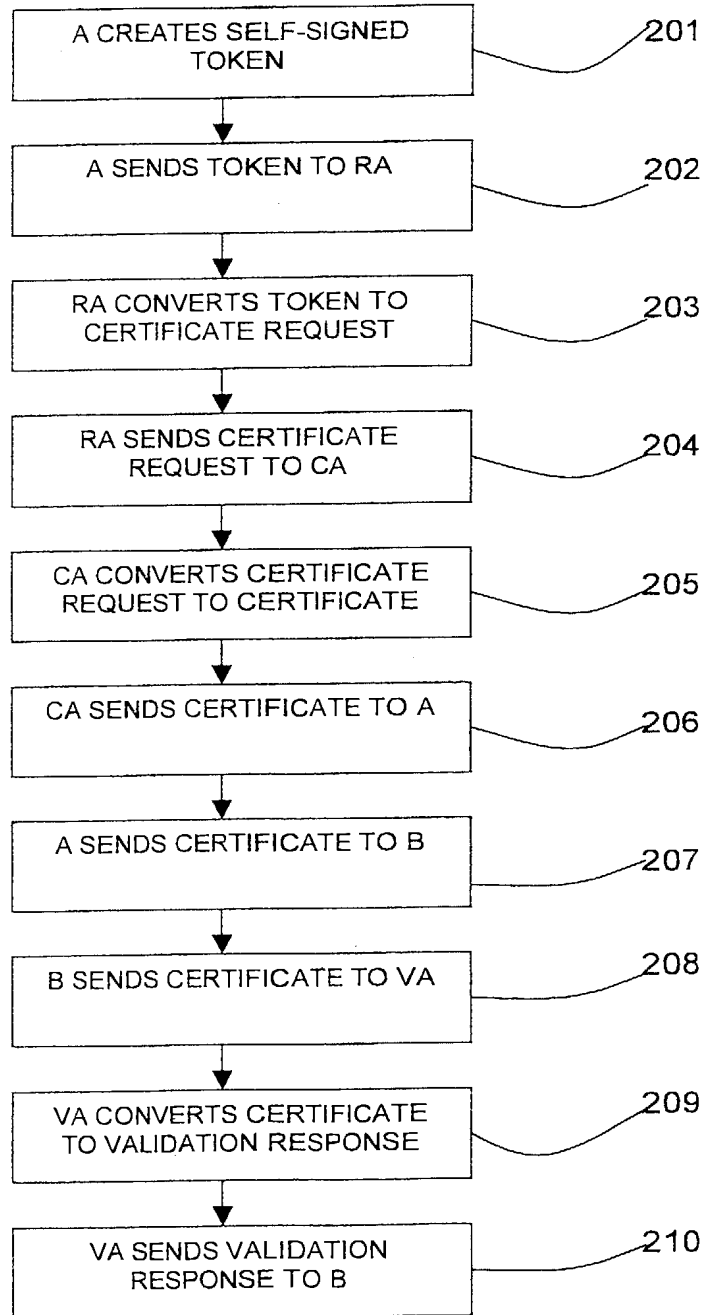


FIG. 3

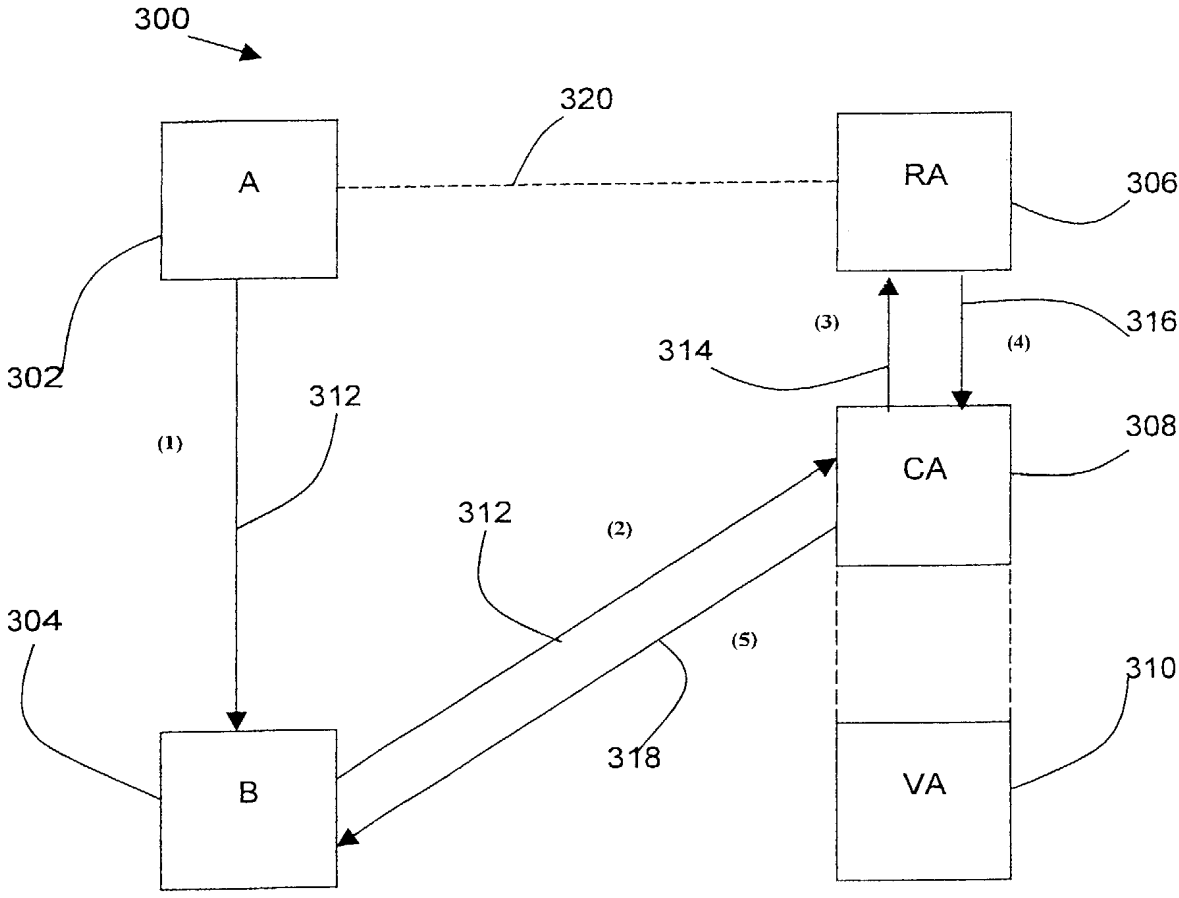


FIG. 4

400 ↘

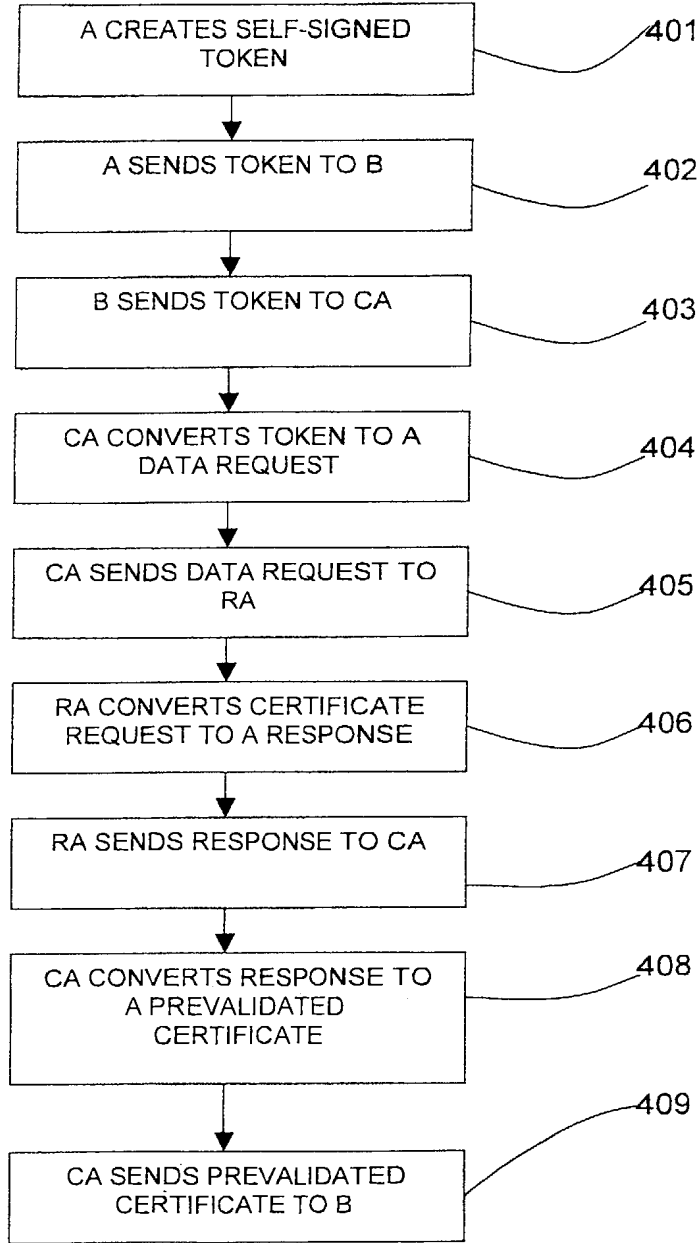
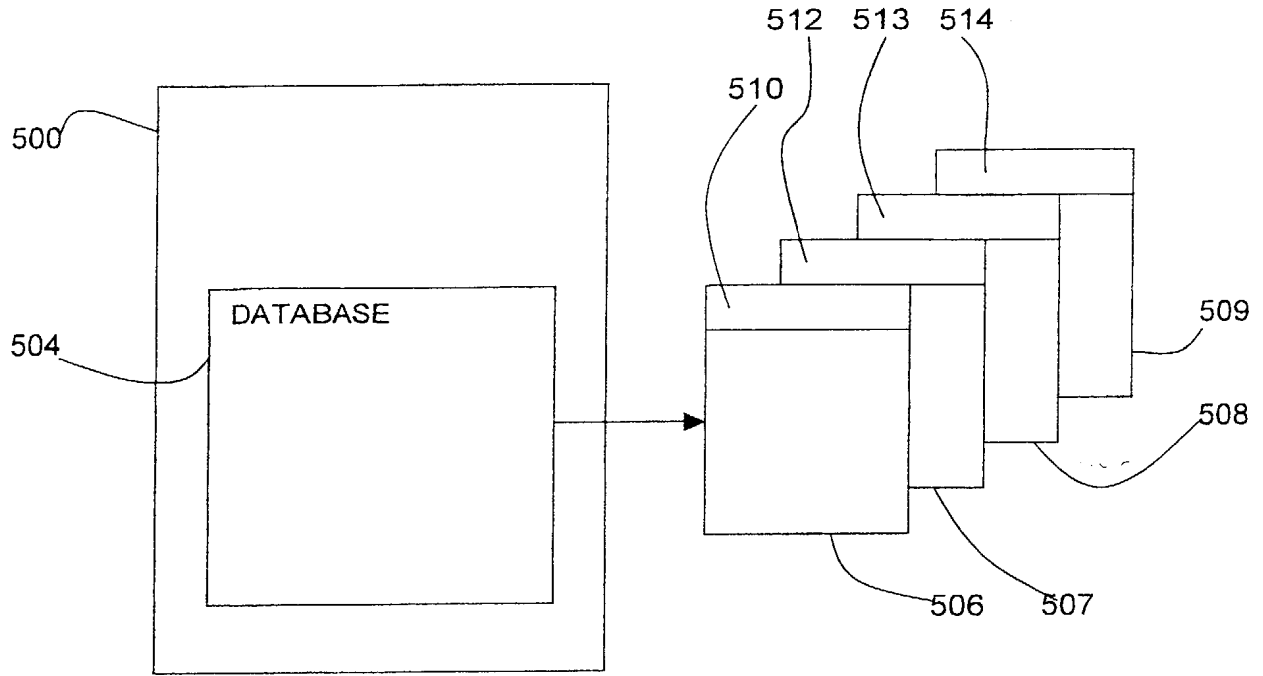


FIG. 5



67

FIG. 6

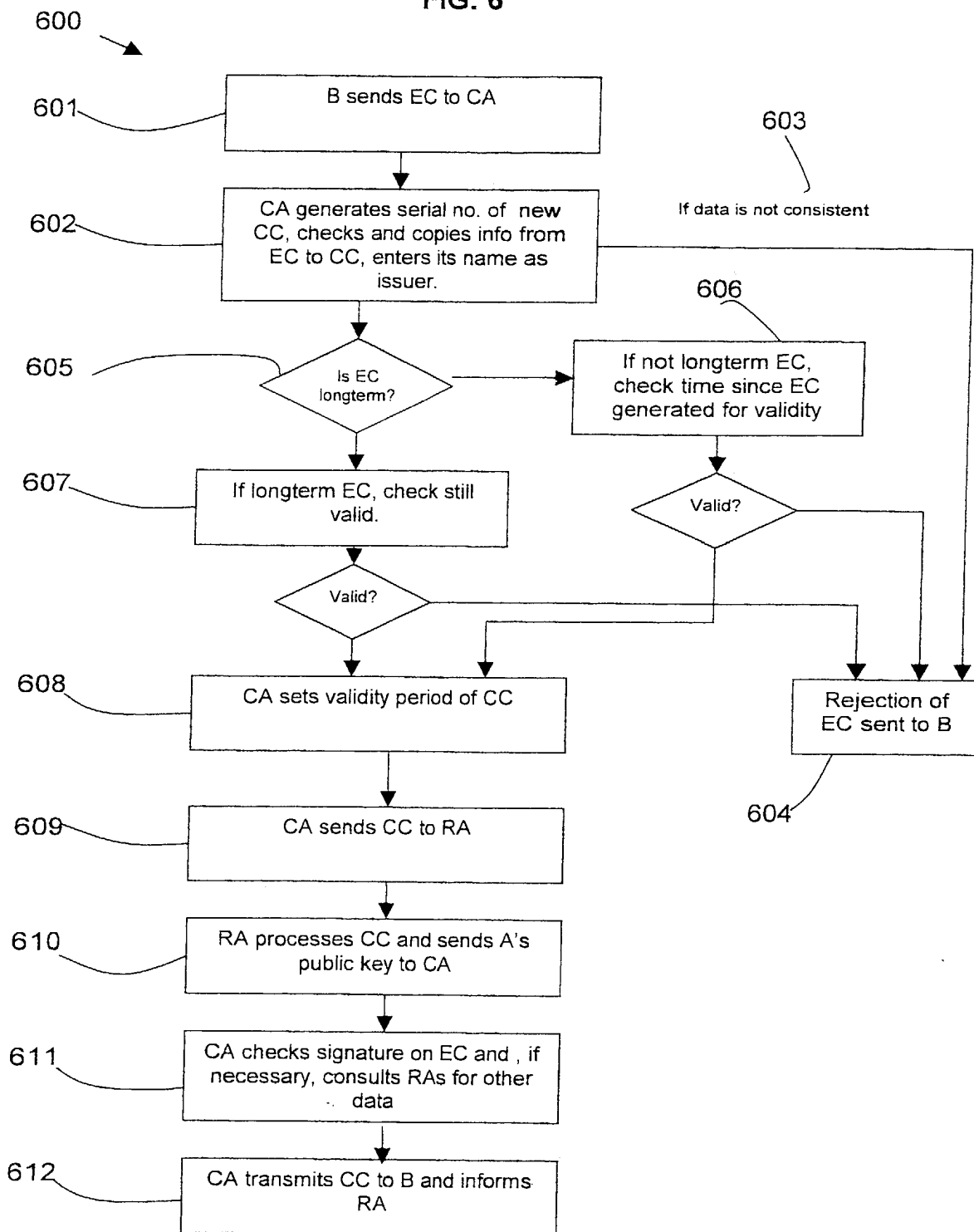
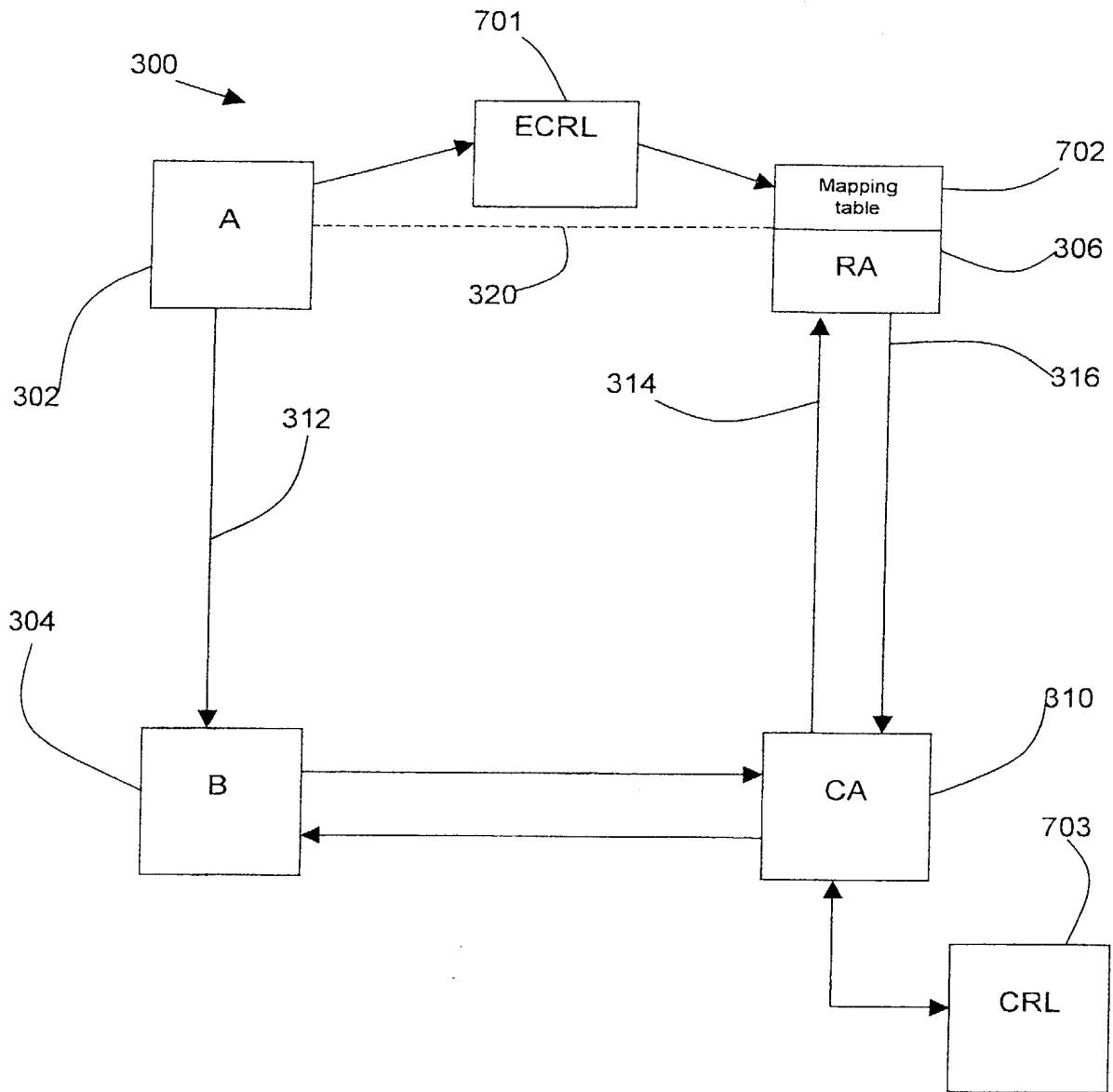


FIG. 7



METHOD AND SYSTEM FOR SUPPLY OF DATA

The invention relates to a method and system for supply of data. This invention also relates to a method for providing a digital signature and digital certificates. The field of the invention is public key cryptography.

Public key cryptography uses an asymmetric algorithm in which the encryption and decryption keys are different and for which it is infeasible to compute one key knowing only the other. Users receive (or, with suitable hardware or software, can generate for themselves) a pair of keys - that is, two large numbers. The user keeps one of these keys private and never discloses it. The other key can be safely made public, just like a phone number or similar personal data. Because of the nature of the algorithm and the way the keys are generated, information encrypted with the private key can only be decrypted with the public key and vice versa. So the sender and receiver do not need to share any secret.

Public key cryptography enables several possibilities:

- Anyone knowing the user's public key can send the user a message encrypted with that key and can be sure that only the user - who alone has the private key - can decrypt it. This provides confidentiality.
- The user might also encrypt a message with his private key. This cannot provide confidentiality, because anyone who knows the public key can decrypt it. But the fact that they can decrypt it means the message must have come from the user - who alone has the private key. This provides integrity and authentication and can also be used as a basis for non-repudiation - the digital equivalent of a signature.
- If a sender signs a message with her own private key and then encrypts it with the recipient's public key, confidentiality, integrity, authentication and non-repudiation are provided together.

In practice, things are actually more complex. In the first example, for performance and operational reasons, the sender will choose a random symmetric session key and use a symmetric cipher to encrypt the message. The public key will be used to encrypt just the session key. Similarly, in the second example, the user will first "digest" the message he wishes to sign, and encrypt the digest with his private key; the recipient will recompute the digest and compare its value with the value he decrypts from the user. A digest is a mathematical construct with a relatively short

fixed length, which is derived from an arbitrarily long message; it has the essential property that it is infeasible, knowing a message and a corresponding digest, to compute another message with the same digest.

5 All the processing is done by software; the real human users do not really "do" any of this.

10 It is important to understand that public keys do not actually have to be published to the world. They can be shared as widely or narrowly as business and privacy requirements dictate.

15 In prior art public keys can be linked together to form a public key infrastructure - a PKI. The links are data structures (or data files) called certificates. Here is how it works:

- Alice may decide to register her public key (and identity information) with a Registration Authority (RA). (In this description of prior art, the usual names "Alice" and "Bob" are used to describe the roles of signatory and relying party, respectively.)
- Using the information collected by the RA, a Certificate Authority (CA) may then create a computer file containing Alice's public key together with information which identifies Alice and a validity period. The CA signs the file with its own private key, creating a certificate.
- A CA's public key may in its turn be certified by another CA; and that CA's certificate will be certified by another and so on until eventually there is a root, that is, an unsigned (or self-signed) public key whose value has to be known some other way.
- So starting from a root it is possible to traverse a certificate chain to discover a public key value.

25
30
35 A set of public keys linked in this way form a public key infrastructure. The simplest PKI has a single CA which acts as the root and which signs all the certificates. It is also possible to build a PKI in prior art using cross-certification instead of a hierarchy, but the end result is broadly the same.

40 Anybody with the right software can be an RA or a CA; whatever the legal or business constraints, there is no technical requirement for an authority to be authorised by anybody.

It is important to understand that the linking of a public key into a PKI does not affect what can be done with the matching private key. Some common misconceptions can be clarified as follows:

- 5 • A certificate is "used" by a relying party, not by a holder of a private key. The relying party extracts from the certificate the public key to be used for encryption or signature checking.

- 10 • A certificate is not needed to create a digital signature or to decrypt a received message.

- 15 • A user does not need to be named in any certificate at all to check someone else's signature or to send them an encrypted message.

- 20 • Not even an Advanced Electronic Signature (as defined in the EU Electronic Signatures Directive) requires a certificate to exist in respect of the matching public key.

A typical method in which a PKI is implemented in prior art is as follows.

- 25 • As well as agreeing to look after her private key, Alice applies her ordinary handwritten signature to a paper application form which references "certificate policies" and "certificate practice statements".

- 30 • Alice then constructs and signs a PKCS#10 object which she sends to her RA. PKCS#10 is an industry standard data format.

- 35 • The RA checks the contents of the received object against what it knows about Alice and sends a certificate request to a CA.

- 40 • The CA signs, and sends to Alice, a certificate upon which any Bob in the world can rely. The certificate will probably have an expiry date a year or so in the future. Alice might have to remember to take action to renew the certificate when it expires, perhaps again using a handwritten signature for that purpose.

- 45 • When Alice digitally signs anything, her software sends the certificate to the relying party along with her signature block and the object that has been signed.

• When Bob receives the transmission, he (that is, his software) first examines the certificate, and checks that it is within its period of validity. If he recognises the "issuer", and knows the issuer's public key, he can also check the signature on the certificate. If it computes, he can extract the public key from the certificate and check the signature on the data that was signed.

• Except, of course, that he might not know the public key of the issuer. He now needs a chain of certificates which link to a public key that he does know. Perhaps Alice sent him the chain, or perhaps he has to search public directories to assemble it himself. He may or may not have to pay a charge to access a directory. Bob needs to process the chain by checking that the issuer name in one certificate is the same as the subject name in the next, that all the signatures on all the certificates check out, and that the validity periods within the chain make sense relative to each other. There is a possibility, of course, that no chain can be constructed which includes both the original certificate and a certificate signed by any public key he knows implicitly.

• Except, of course, that the original certificate, or any of the certificates in the chain, may have been revoked. So Bob's software must now go in turn to an Internet address (URL - Uniform Resource Locator) included in each certificate, extract the most recent certificate revocation list (CRL) from that URL, and check that the serial number of the next certificate in the chain does not appear. He may or may not have to pay a charge for access to each CRL.

• As an alternative to the last three bullets, Bob can instead pass the certificate to a validation authority (VA) which will do much of the work for him, and return to him a signed go/no-go response on the validity of the original certificate. If validation services are sufficiently integrated, they may be able to succeed more often than Bob alone could. Use of a validation service will probably be chargeable.

• Bob archives the certificate of interest and either the rest of the chain and the CRLs or the signed validation response. To guard against later revocation of Alice's certificate, Bob would also do well to get from a timestamp authority a timestamp of the signature block on the signed data to prove that he had it in his possession before the revocation occurred.

Ever since the invention of public key cryptography, the vision has been held out of a universal infrastructure that would enable everyone in the world to verify with assurance the digital signatures of everyone else. Electronic transactions exploiting this infrastructure would acquire the important properties of integrity and non-repudiation.

Achievement of the vision would empower individuals because they could digitally sign anything, anywhere, any time. And it would consequently deliver business competitiveness - a typical company, already participating in one e-marketplace as a buyer perhaps, could smoothly enter another, perhaps as a seller, with the same identity. This vision has the potential to alter the nature - and the economics - of the e-marketplace concept. The whole world could develop rapidly into a single e-marketplace - an integrated e-economy.

The prior art does not easily enable subjects to participate in a public key infrastructure with an ability to sign anything, anywhere. Key-pairs in the prior art are generally seen as part of a "managed identity" rather than an extension of personality, independent of certification.

The prior art PKI is largely relevant only in a managed identity context in which a subject is related directly with a single affiliate and the identity only makes sense within that context. For example, an affiliation as an employee, as a customer of a bank, or as a vendor to a major corporation etc. Having acquired or generated a key-pair, the subject convinces a single business partner (a bank, for example, or an employer, or a major customer) of the binding of the subject's identity to its public key. Any particular individual would be likely to have multiple managed identities outstanding at any one time.

A further major problem with the prior art in delivering the universal infrastructure vision is that the CA's contract is typically with the subject and not with the relying party. There is a realisation among traditional CA businesses that the subject will be unwilling to pay the full cost - or perhaps any part of the cost - of "being issued with a certificate".

There is a furthermore a perverse liability issue which arises from the fact that the CA's contract is with Alice - the subject named in the certificate - and not with Bob - who relies on its correctness. In prior art PKI any per-certificate liability is unbounded, because whoever signed the certificate never gets to know who is relying on it until there is a problem. Alice can send the same certificate to a million Bobs and the CA will never know how much liability is building up. The "value" of a

certificate can be reused and reused without the CA (the source of that value) ever becoming aware.

Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures ("the Directive") defines a number of the terms used in the present document. However, the definition of "certificate" is wider in the present document than in the Directive; the Directive's use of this word corresponds to the use in the present document of the term "verification certificate". The term "digital signature" in the present document is a technique for implementing the Directive's notion of an "advanced electronic signature".

According to a first aspect of the present invention there is provided a method for supply of data relating to a described entity to a relying entity comprising: generating a first digital certificate signed with an electronic signature by a first signing entity and including: one or more attributes of the described entity; one or more attributes of the first digital certificate which include one or more attributes identifying the first signing entity; an indication of data relating to the described entity which is to be supplied; an indication of one or more sources for the data to be supplied; and one or more attributes identifying one or more relying entities to which the data is to be supplied; the relying entity forwarding the first digital certificate for processing; a source supplying the data indicated in the first digital certificate.

The first digital certificate empowers the relying entity to gain access to the personal data of the described entity which may be held by a source in a data store and may be referred to in this document as an empowerment certificate. The described entity and the relying entity may be individuals, groups of individuals, individuals in a particular role, corporations, organisations, computer applications or systems, automated machines, etc.

Electronic signatures are defined in the Directive as data in electronic form which is attached to or logically associated with other electronic data and which serves as a method of authentication.

The first digital certificate may include any data which the relying entity has previously requested to be included such as a reference, nonce or other data.

A source can hold data or can refer to one or more data sources.

The first digital certificate may be sent with an object signed with a digital signature, but could also be sent on its own. The signing entity

of the first digital certificate may be the described entity such that the first digital certificate is a form of self-signed certificate. If an object signed with a digital signature is sent with the first digital certificate, the digital signature and the electronic signature in the first digital certificate may use different key pairs for signing.

The data relating to the described entity may include one or more public keys corresponding to private keys controlled by the described entity.

The data relating to the described entity may be supplied by means of a second digital certificate to the relying entity, the second digital certificate signed with an electronic signature by a second signing entity and including: one or more attributes of a described entity including the data which is to be supplied; one or more attributes of the second digital certificate which include one or more attributes identifying the second signing entity; and one or more attributes identifying one or more relying entities to which the data is to be supplied.

The second digital certificate may be referred to in this document as a custom certificate. The first and second digital certificates may be in the format prescribed by international and industry standards for certificates with the electronic signature using public key cryptography. The first and second digital certificates may include attributes which are sufficient to identify the described entity as well as the relying entity. These may be a single attribute or a combination of more than one attribute. For example, a name may not be sufficient to identify uniquely an entity, whereas a combination of a name, a date of birth and an address will often uniquely identify the entity.

The first digital certificate may authorise the relying entity to use the first digital certificate to obtain a second digital certificate. The relying entity may be authorised to obtain a second digital certificate which is marked as qualified. "Qualified certificates" are defined in the Directive.

The second digital certificate may include one or more attributes of the first digital certificate. At least some of the contents of the first digital certificate may be copied to the second digital certificate.

The method may include the relying entity forwarding the first digital certificate to an intermediate entity to obtain data from a source. The intermediate entity may provide a service for the relying entity and may provide insurance and take financial liability for the supply of the data

from the source. The intermediate entity may generate the second digital certificate.

5 The second digital certificate may include one or more attributes identifying the relying entity which are different from the one or more attributes identifying the relying entity included in the first digital certificate.

10 The second digital certificate may include one or more attributes identifying the described entity which are different from the one or more attributes identifying the described entity included in the first digital certificate.

15 The described entity may generate a digital signature using a private key with a corresponding public key and the first signing entity may include the digital signature or a cryptographic digest thereof in the first digital certificate and the data to be supplied to the relying entity may include the public key. A cryptographic digest may be obtained using a hash function. Once the indicated data, including the public key, is
20 received by the relying entity from the source, the digital signature can be verified.

25 The first digital certificate and the second digital certificate may include a period of validity. The period of validity of the first digital certificate or the second digital certificate may be that short period of time during which a digital signature was generated. For example, this may be 1 or 2 seconds. A digital certificate can be generated with a validity period which begins prior to the generation of the digital certificate. The period of validity may be in the past, prior to the generation of the
30 digital certificate, or in the future or for a period spanning the past and the future.

35 The data indicated in the first digital certificate may include confirmation of a payment or a debt due from the described entity identified in the first digital certificate to the relying entity identified in the first digital certificate. A second signing entity may indicate in a second digital certificate a guarantee of a debt indicated as due in a first digital certificate.

40 A change in previously supplied data may be indicated by the supply of a list identifying a second digital certificate relating to the previously supplied data. A list may identify a first or second digital certificate specifying data which is no longer authorised to be supplied to the relying entity. The generation of the list may include one or more attributes

identifying relying entities to which the list relates. The list may be a certificate revocation list.

5 The method may include generating and storing a list for the second digital certificates, which is indexed by one or more attributes identifying relying entities such that all second digital certificates in the list relevant to a relying entity can be identified.

10 According to a second aspect of the present invention there is provided a system for supply of data relating to a described entity to a relying entity, the system comprising: a first signing entity application, a relying entity application and a data store wherein the data store holds data relating to the described entity; the first signing entity application has means for generating a first digital certificate signed with an
15 electronic signature by the first signing entity application and including: one or more attributes of the described entity; one or more attributes of the first digital certificate which include one or more attributes identifying the first signing entity; an indication of data relating to the described entity which is to be supplied; an indication of one or more
20 sources for the data to be supplied; and one or more attributes identifying one or more relying entities to which the data is to be supplied; the relying entity application has means for forwarding the first digital certificate for processing; and means for supplying the data indicated in the first digital certificate from the data store.

25 The system may be provided using a secure messaging system across a network, for example the Internet. The described entity and the relying entity may use software applications to generate and sign messages and certificates. The data to be supplied may be held in a data store by a
30 source and the data store may be an electronic database. A source may hold the data store or may refer to one or more further sources. The first signing entity may be the described entity. The system may include more than one data store holding data relating to the described entity.

35 The first digital certificate may include any data which the relying entity has previously requested to be included such as a reference, nonce or other data.

40 A second digital certificate may be provided for supplying the data relating to the described entity to the relying entity application, the second digital certificate signed with an electronic signature by a second signing entity application and including: one or more attributes of the described entity including the data which is to be supplied; one or more attributes of the second digital certificate which include one or more

attributes identifying the second signing entity; and one or more attributes identifying one or more relying entities to which the data is to be supplied.

5 The first digital certificate may authorise the relying entity to use the first digital certificate to obtain a second digital certificate. The relying entity may be authorised to obtain a second digital certificate which is marked as qualified. The second digital certificate may include one or more attributes of the first digital certificate. At least some of the contents of the first digital certificate may be copied to the second
10 digital certificate.

The system may include an intermediate entity application to which the relying entity application forwards the digital certificate to obtain data from the data store. The intermediate entity may use a software
15 application to act between the relying entity and a source. An intermediate entity application may generate the second digital certificate.

20 The second digital certificate may include one or more attributes identifying the relying entity which are different from the one or more attributes identifying the relying entity included in the first digital certificate.

25 The second digital certificate may include one or more attributes identifying the described entity which are different from the one or more attributes identifying the described entity included in the first digital certificate.

30 The described entity may generate a digital signature using a private key with a corresponding public key and the first signing entity may include the digital signature or a cryptographic digest thereof in the first digital certificate and the data to be supplied to the relying entity may include the public key. A cryptographic digest may be obtained using a hash function. Once the indicated data, including the public key, is
35 received by the relying entity from the source, the digital signature can be verified.

40 The first digital certificate and the second digital certificate may include a period of validity. The period of validity of the first digital certificate or the second digital certificate may be that short period of time during which a digital signature was generated. A digital certificate can be generated with a validity period which begins prior to the generation of the digital certificate. The period of validity may be in

the past, prior to the generation of the digital certificate, or in the future or for a period spanning the past and the future.

5 The data indicated in the first digital certificate may include confirmation of a payment or a debt due from the described entity identified in the first digital certificate to the relying entity identified in the first digital certificate. A second signing entity may indicate in a second digital certificate a guarantee of a debt indicated as due in a first digital certificate.

10 A change in previously supplied data may be indicated by the supply of a list identifying a second digital certificate relating to the previously supplied data. A list may identify a first or second digital certificate specifying data which is no longer authorised to be supplied to the relying entity. The generation of the list may include one or more attributes identifying relying entities to which the list relates. The list may be a certificate revocation list.

20 The data store may have a means of determining for an item of data included in the data store information concerning or contained in a first digital certificate which has referenced that item, or information concerning or contained in a second digital certificate which provides the value of that item. The certificate lists just described may be generated through this means.

25 The intermediate entity application may include a storage means for storing second digital certificates referenced by the relying entities identified in the second digital certificates.

30 The system may include a proxy entity application to which the relying entity application or the intermediate entity application may forward the first digital certificate to obtain information specifying to which data store or other proxy entity application the first certificate should next be forwarded.

35 According to a third aspect of the present invention there is provided a computer program product stored on a computer readable storage medium, comprising computer readable program code means for performing the steps of: generating a digital certificate signed with an electronic signature by a signing entity and including: one or more attributes of a described entity; one or more attributes of the digital certificate which include one or more attributes identifying the signing entity; either an indication of data relating to the described entity which is to be supplied and an indication of one or more sources or the data itself; and one or more

40

attributes identifying one or more relying entities to which the data is to be supplied.

5 A computer program product may be provided with one or more of the features of the first and second aspects of the present invention.

10 According to a fourth aspect of the present invention there is provided a digital certificate signed with an electronic signature by a signing entity and comprising: one or more attributes of a described entity; one or more attributes of the digital certificate which include one or more attributes identifying the signing entity; either an indication of data relating to the described entity which is to be supplied and an indication of one or more sources or the data itself; and one or more attributes identifying one or more relying entities, wherein the relying entities are entities to which the data relating to the described entity is to be supplied.

15 The digital certificate identifying the relying entity may be authorising the relying entity to obtain the indicated data relating to the described entity or may be supplying the data itself to the relying entity.

20 The digital certificate may be provided with one or more of the features of the first and second aspects of the present invention.

25 According to a fifth aspect of the present invention there is provided a method of providing a digital signature based on a digital certificate comprising: generating a digital signature using a private key corresponding to a public key, the signed data including: one or more attributes identifying a digital certificate to be generated; generating a digital certificate signed with an electronic signature by a signing entity and including: one or more attributes of a described entity which are sufficient to obtain the public key; one or more attributes of the digital certificate which include one or more attributes identifying the signing entity; and an indicated period of validity of the digital certificate which begins earlier than the time of generation of the digital certificate; wherein the digital certificate is generated after the generation of the digital signature.

30 An object may be signed with a digital signature which forward references a digital certificate which has not yet been generated and then a digital certificate may be generated which references back to the digital signature and has a period of validity which includes the time of the generation of the digital signature.

More than one digital signature may be generated which identifies the same digital certificate. The signing entity may be the described entity.

5 The period of validity of the digital certificate may be that short period in which the digital signature was generated.

10 The one or more attributes identifying the digital certificate to be generated given in the digital signature may include a serial number. The lowest available serial number which can be used for the next digital certificate to be generated or the last used serial number using each private key may be recorded.

15 According to a sixth aspect of the present invention there is provided a system for providing a digital signature based on a digital certificate, the system comprising:

20 a described entity application with means for generating a digital signature using a private key corresponding to a public key, the signed data including: one or more attributes identifying a digital certificate to be generated; a signing entity application having means for generating a digital certificate with an electronic signature and including: one or more attributes of a described entity which are sufficient to obtain the public key; one or more attributes of the digital certificate which include one or more attributes identifying the signing entity; and an indicated period of validity of the digital certificate which begins earlier than the time of generation of the digital certificate; wherein the digital certificate is generated after the generation of the digital signature.

25 A system may be provided with one or more of the features of the fifth aspect of the present invention.

30

35 According to a seventh aspect of the present invention there is provided a computer program product stored on a computer readable storage medium, comprising computer readable program code means for performing the steps of: generating a digital signature using a private key corresponding to a public key, the signed data including: one or more attributes identifying a digital certificate to be generated; generating a digital certificate signed with an electronic signature by a signing entity and including: one or more attributes of a described entity which are sufficient to obtain the public key; one or more attributes of the digital certificate which include one or more attributes identifying the signing entity; and an indicated period of validity of the digital certificate which begins earlier than the time of generation of the digital certificate; wherein the digital certificate is generated after the generation of the digital signature.

40

A computer program product may be provided with one or more of the features of the fifth aspect of the present invention.

5 According to a eighth aspect of the present invention there is provided a digital certificate signed with an electronic signature by a signing entity and comprising: one or more attributes of a described entity; one or more attributes of the digital certificate which include one or more attributes identifying the signing entity; and an indicated period of validity of the digital certificate which begins earlier than the time of generation of the digital certificate.

The indicated period of validity of the digital certificate may end no later than the time of generation of the digital certificate such that the period of validity of the digital certificate is all in the past.

15 Alternatively, the period of validity may extend from the past to a future time.

The described entity may be the signing entity such that the digital signature is a form of self-signed certificate. The electronic signature may use public key cryptography. The digital certificate may include a time stamp indicating the time of generation.

20 According to a ninth aspect of the present invention there is provided a digital signature using a private key corresponding to the public key derived from a digital certificate as defined in the eighth aspect of the present invention, wherein the digital certificate is generated after the generation of the digital signature, the signed data including: one or more attributes identifying the digital certificate to be generated.

25 The proposed "empowerment infrastructure" which can be implemented through the invention describes a public key infrastructure (PKI) in the sense that it provides for a relying party to establish the value of a public key matching the private key held by an identified subject, and in the sense that it extends the prior art constructs of PKI, including certificates and certificate revocation lists (CRLs) signed by certificate authorities (CAs). The invention itself relies on public key cryptography, but fundamentally challenges the conventional wisdom about the role of keys and certificates in a workable PKI model.

30 The empowerment approach that the invention enables goes well beyond the possibilities of PKI prior art to allow a wide range of personal data items - not just public keys - to be certified within a privacy enhancing framework that empowers the subject to control who can access his personal data, and how and when. The invention enables a method of delivering, not

just public keys, but any piece of assured personal data. In other words, an architecture for an e-marketplace which brings together the buyers and sellers of personal data. The brokers of this marketplace are the data subjects themselves; no personal data moves in the empowerment
5 infrastructure except with the explicit authorisation of the subject to whom that data relates.

The invention also provides a payments mechanism integrated into the personal data framework. Imagine the sale, empowered by Alice, of a piece
10 of personal data of the form "Alice is indeed able to pay you the sum of 100". Usually, when personal data is sold, the database from which it is derived is not altered. But this case has to be an exception, and some database attribute, controlled by the seller of Alice's personal
15 information, has to be altered by exactly - or, where commission or interest are involved, approximately - one hundred. It now just takes a small leap of imagination to see a payment as simply a piece of personal data that changes when it is sold. So the invention also permits a secure
20 payments architecture. By extension, it is also possible to use the infrastructure to confirm a debt due from the signatory to the relying party, and even to indicate a guarantee for such a debt.

Embodiments of the invention are now described, by means of examples only, with reference to the accompanying drawings in which:

25 Figure 1 is a diagram of a system of delivery of data of the prior art;

Figure 2 is a flow diagram of the system of Figure 1;

30 Figure 3 is a diagram of a system of delivery of data in accordance with the present invention;

Figure 4 is a flow diagram of the overall system of Figure 3;

35 Figure 5 is a diagrammatic representation of part of the system in accordance with the present invention;

Figure 6 is a flow diagram of part of the system of Figure 3; and

40 Figure 7 is a diagram of a system in accordance with the present invention.

Referring to Figure 1, the traditional system of delivery of a data object in the form of a certificate as known from the prior art is shown. Figure

1 shows a first user of the system, Alice 102, and a second user, Bob 104. There are also provided a registration authority (RA) 106, a certification authority (CA) 108 and a validation authority (VA) 110.

In the prior art system, the data object to be delivered is a certificate for use in public key cryptography. In public key cryptography, a public key certificate associates a public key value with the certificate's subject. The certificate's subject is a particular person, role, device or other entity that controls the corresponding private key.

A public key certificate is digitally signed by a person or entity called a certification authority.

A registration authority (RA) traditionally manages interactions between a certification authority (CA) and its subscribers or certificate applicants. There may be multiple RAs for a CA. The issuance of a certificate may involve a personal presence for verifying the applicant's identity through presentation of identifying documents. The RA does not itself issue the certificates but may validate, approve or reject certificate applications.

In prior art, the method of delivering a certificate starts with Alice's self-signed token (PKCS#10) 112. PKCS#10 defines a format for a message to request the issuance of a certificate from a CA. The PKCS#10 token 112 allows the requesting entity, Alice 102, to supply her public key and other values requested for inclusion in the certificate. Alice 102 sends the token 112 to the RA 106, which converts it to a certificate request 114. The certificate request is sent by the RA to the CA 108. The CA 108 converts it to a certificate 116 which it sends to Alice 102. Alice 102 sends the certificate 116 unchanged to Bob 104. Bob then sends the certificate unchanged to a validation authority (VA) 110, which converts it to a validation response 118 to Bob 104. Figure 1 shows the order of these actions in numbers given in parentheses.

Figure 2 shows a flow diagram of the traditional system 200 of the prior art described above. Alice creates a self-signed token in the first step 201 and sends this 202 to an RA. The RA converts the token to a certificate request 203 and sends 204 the certificate request to a CA. The CA converts the certificate request to a certificate 205 and sends 206 the certificate to Alice. Alice sends 207 the certificate to Bob. Bob need to have the certificate validated so he sends the certificate to a VA 208. The VA converts 209 the certificate to a validation response either confirming or denying that the certificate is valid. The validation response is sent by the VA to Bob 210.

In a described embodiment of the present invention, a method and system are referred to as an empowerment method or system. This system is shown in Figure 3 using the same structure as Figure 1 for comparison purposes. The embodiment is described in terms of delivery of a certificate for use in public key cryptography; however, as will become evident, the present invention is not restricted to the delivery of certificates only for this particular use. Alice 302 is a described entity and Bob 304 is a relying entity.

Referring to Figure 3, Alice 302 has previously registered 320 with an RA 306 and the RA 306 has information about Alice 302. Alice 302 sends a self-signed token 312 to Bob 304. Bob 304 sends the token 312 unchanged to a CA 308. The CA 308 converts the token to a request 314 to one (or more) RAs 306. The RA 306 converts the request to a response 316 to the CA 308. The CA 308 converts it to a pre-validated certificate 318 which it sends to Bob 304. As the certificate is pre-validated, Bob 304 does not need the explicit services of a VA to validate the certificate. The functions of the VA 310 are combined with the CA 308. Figure 3 shows the order of these actions by numbers in parentheses.

The method 400 of the described embodiment is shown in a flow diagram in Figure 4. In the first step 401 Alice creates a self-signed token. Alice sends 402 the token to Bob. Bob sends 403 the token to a CA. The CA converts 404 the token to a data request and sends 405 the request to a RA. The RA converts 406 the request to a response and sends 407 the response to the CA. The CA converts 408 the response to a pre-validated certificate and sends 409 the pre-validated certificate to Bob.

The traditional system of the prior art and the described embodiment of the system both execute three conversions. Both systems start with Alice self-signing a token and end with Bob possessing a validated certificate naming Alice as subject. But the Alice-to-Bob portion is the first of five steps in the empowerment system of the described embodiment and the fourth of six steps in the traditional system.

This difference of sequence turns out to have far-reaching consequences. In the empowerment system 300, Alice 302 can choose at the granularity of each transaction which of her identities (as employee, taxpayer, bank customer, pseudonym, ...) to assert and which of her attributes (items of personal data) to empower her RA 306 - or RAs - to disclose. Since Bob 304 is now in the customer role with the CA 308, the certificate policy reflects what he is willing to pay, enabling an improved PKI business model in which liabilities are understood and controlled. Because there is no requirement for a certificate to exist before Alice makes her first ever

signature, she can sign her RA agreement digitally rather than in handwritten form.

5 The empowerment system 300 shifts mindset away from the notion of a certificate as part of a managed identity towards a mechanism through which a data subject (Alice 302) empowers an RA to reveal validated personal data to a relying party (Bob 304). A public key value becomes just another piece of validated personal data delivered through this process.

10 The empowerment system of the described embodiment is now considered in more detail.

15 THE DATABASE

The described embodiment of the empowerment system assumes that personal data is held in databases at one or more sources. (The term database is taken to include directories.) Databases model what is going on in the real world. A change in a database reflects a change in the real world. 20 The embodiment only applies to those database entries which identify the subject- that is, where there is sufficient information in the entry to distinguish the subject from all other subjects in that database. There is no requirement that databases must be digital - hardcopy databases are included.

25 Generally, there can be expected to be more than one way to identify a subject. The following is an imagined extract from Alice Earthling's entry in the personnel database of her employer Acme SA:

30 Name

Alice Earthling

35 Date of birth

19631117

Home address

40 65 Southview Road

Employee number

45 65193

Alice's unique number at the Internal Revenue Service (Acme hold this information to pay withholding tax)
DF456781A

5

Alice's banker
Rutland Bank

10

Alice's bank account number (Acme hold this information in order to pay Alice each month)
01081208

15

Alice's work e-mail address
alice.earthling@acme.com

20

Alice's home e-mail address
Alice@earthling.name

25

Alice's work phone number
+99 12 3000 3274

30

Alice's cellphone number
+99 73 0578 2407

35

Alice's home phone number
+99 13 2553 8109

Alice's registered domain name
alice.earthling.name

40

The value of the public key matching the private key under Alice's control
956DF57E4...

45

A JPEG file containing a full face photograph of Alice
AD53827D5C88E575EAB6678...

A TIFF file containing a digitised image of Alice's handwritten signature
FE4368AB543C55FDE653FB6...

A pseudonym
756384928475

5

Alice's salary
60,500

10

Alice's external purchasing limit at Acme
100,000

15

The data in the database entry for Alice Earthling includes attributes which provide identification, authentication, location and authorisation. Note that a pseudonym is permitted as an identifier.

20

As the Alice/Acme example includes several data items, it is possible to take several views of the entry, each with a different identifier. So for each view there is a primary identifier and a predicate. The predicate contains all the attributes of the entry except those in the primary identifier which characterise the view. It might be necessary to use a combination of attributes (for example, bank and account number) to construct a single primary identifier, or a single attribute (for example, personnel number) might suffice. In the example, Alice's salary will always be part of the predicate. Her work e-mail address will be part of the predicate in all views except one, namely the view which has her work e-mail address as the primary identifier.

25

30

Note that the possibility of the public key value being a primary identifier is allowed for - making the practical assumption that the same key pair will never be generated twice.

35

This description is for the general case. The system also allows for the simpler case of an entry which has only one possible view because it has only one attribute or set of attributes that could be a primary identifier.

40

Databases of the form just described already exist pervasively throughout the world in government departments and agencies, large corporations and most other sorts of organisation.

THE CERTIFICATE

45

One way of storing data about individuals is in the form of certificates. In the described embodiment, in respect of individuals, a certificate can be seen as a digitally signed extract of an entry in a database. This can

be extended further to include certificates relating to entities that are not individuals. In the described system, certificates are the mechanism through which entries become visible outside the organisation operating each database.

5 A certificate in the described embodiment must contain information from a single view of a single entry. As will be described later, it may also contain other information. This is a crucial difference between a certificate and a database entry. A database entry sits there with all views equally possible. In a certificate, the identifier is committed to a
10 single view.

A certificate must contain the full primary identifier relating to the selected view. The identifier in a certificate is called the "distinguished name". A certificate may also contain information from the predicate of
15 the selected view, either the whole predicate or any sensible subset of it. There little value in a certificate that contains only a distinguished name.

In particular, the predicate information may contain authenticators
20 (including, public key values), locators, authorisers and non-primary identifiers.

Where one or more non-primary identifiers are included, they may be useful as a redundancy checking mechanism. For example, in a certificate which
25 has a bank account number as the primary identifier, one or more of the other identifiers (common name, say) can be used by the bank to double-check against mis-identification.

A traditional certificate known from the prior art identifies a subject or
30 described entity but does not identify any particular relying party or entity. A relying entity is a user of a certificate, that is, someone who relies on the accuracy of the contents of the certificate.

The model's taxonomy then develops as follows:

- 35
- A certificate containing as authenticator a public key which matches a private key used for creating digital signatures is classed as a verification certificate.
 - Verification certificates are either issued to the public, or not, and either qualified or not. The difference is important because the European Union Electronic Signatures Directive treats each class differently.
- 40

• The model assigns certificates to one of three further classes. The classes are traditional, empowerment and custom. Further information on these classes appear later, but in summary:

- A traditional certificate identifies a subject but does not identify any particular relying party. A relying party is a user of a certificate, that is, someone who relies on the accuracy of the contents of the certificate. This class of certificate is found extensively in prior art.
- A custom certificate identifies both a relying party and a subject, and the entity who signs the certificate is not the subject of the certificate.
- An empowerment certificate identifies both a relying party and a subject, and is signed by the subject.

Empowerment and custom certificates are either instantaneous or long term. (Traditional certificates are always long term.) The period of validity of an instantaneous certificate is short enough to practically prevent more than one signature being created in that time with the same private key. It is possible to create many such signatures with the same private key during the period of validity of a long term certificate.

In the model all empowerment and custom verification certificates are classed as issued to the public. In the model custom certificates can be either qualified or unqualified while empowerment certificates can never be qualified.

THE REGISTRATION AUTHORITY

The traditional notion of a registration authority (RA) persists in the described system in the form of sources for data to be supplied. In the embodiment, the registration authority for a given subject is defined as:

- The controller of a database...
- who has agreed with the subject to become an RA in respect of the subject ...
- and includes in its database entry for the subject the value of the subject's public verification key.

In respect of a given subject, an RA is either a direct RA (DRA) or an indirect RA (IRA). The difference is as follows:

- 5 • A direct RA holds the value of the subject's public key as primary data, updating it in accordance with events in the real world. To achieve this, a DRA probably has some sort of contract with the subject to cover notification in the case of loss or compromise of the corresponding private key.
- 10
- An indirect RA has cached a longterm custom certificate which contains the value of the public key, and has access to a current certificate revocation list (CRL) which enables the continuing validity of such a certificate to be checked. (CRLs are explained
- 15 further below.)

The same organisation might be a DRA in respect of one subject and an IRA in respect of another.

20 No subject can have an IRA without also having at least one DRA, although it is possible for a subject to have a DRA and no IRAs. This is because there must be somewhere in the infrastructure where the public key value is bootstrapped. Unless a subject had a DRA in the first place, there could be no longterm custom certificates for any IRA to cache. If a subject

25 stopped having a relationship with its last DRA, then it is likely that all the relevant longterm custom certificates would very soon appear in the CRLs which the IRAs check, so very quickly the subject would cease to have any IRA relationships either.

30 There is nothing in the described system which prevents a subject having more than one DRA - either because the subject has more than one key pair or because one or more key pairs are tracked by one or more DRAs.

 The mechanism through which the DRA is sure of the subject's public key value is outside the description given here and is not part of the

35 invention. There are however plenty of examples in prior art of how this relationship can be implemented. In fact, any RA - DRA or IRA - has to have some method of establishing the value of all the data items it holds "for real" on each subject, not just the public key. Again, there is a

40 mass of existing prior art in this area. ("For real" means "not in a certificate signed by somebody else".)

The correct operation of this unspecified mechanism is axiomatic to the whole model. Everything that happens elsewhere in the model depends on this part being done correctly.

5 Figure 5 shows a representation of the RA 500 of the described system. The RA holds a database 504. 506, 507, 508, 509 are single views of the database. Each view 506, 507, 508, 509 has a distinguished name 510, 512, 10 513, 514 for that view which is the primary identifier. The views 506, 507, 508, 509 can also include attributes from the predicate of the selected view of the database, including public key values, locators, 15 authorisers, etc.

In the described system, RAs have the following capabilities.

15 An RA (of either class), in its role as a database controller, can maintain and process the data it holds on each subject for whatever reason it is, apart from being an RA, that it holds that data. So, for example, the personnel department of Alice Earthling's employer Acme will continue to process the monthly payroll against the employee database.

20 An RA (of either class) can receive and process entry updates digitally signed by the subject. The RA knows the subject's public key (either because, as a DRA, it is tracking it or, as an IRA, because it can validate the cached certificate against the CRL), so it is always able to check the signature.

25 Importantly, an RA can send a message to a certificate authority (CA) which can result in the CA signing or revoking a digital certificate.

30 The described system predicts that many organisations - and perhaps most organisations within the public sector - will become RAs. In such cases, being an RA will be incidental to being something else. There is no specific requirement in the system for organisations whose whole business mission is that of an RA, although such organisations are obviously possible.

35

THE SIGNING DEVICE

40 The model abstracts a digital signature to the operation of a finite state machine called a signing device. The signing device has access to a source of local time which corresponds to the usual standards notion of GeneralizedTime and which increments with a granularity of one second. The state of the machine is defined by:

- the value of a key pair, which can change from time to time;
- the value of an empowerment certificate serial number, which is an integer that increases before or after each signature operation; and

- 5 • (optionally) by a set of values that enable intelligent guesses to be made of data to be included in an empowerment certificate.

How the machine and its state are implemented is not defined in the model and are not part of the invention, but it may prove helpful to think of a smart card or a wireless device. There are minor privacy advantages in
10 incrementing the serial number by amounts other than unity to obfuscate the rate at which Alice is effecting signing operations.

A signing operation might proceed as follows:

- 15 • The device takes the value of the local time.
- The device increments the empowerment certificate (EC) serial number.
- 20 • For each of zero or more objects to be signed in turn it displays each object to Alice, and receives from her a decision whether or not to sign.
- For each object that Alice wants to sign, if any, the device
25 computes a signature block over a data structure consisting of:
 - the object to be signed;
 - a reference, by serial number and the hash of Alice's
30 public key value, to the EC about to be created; and
 - possibly other information.
- The device then displays an EC confirmation screen with
35 intelligent guesses of the values to be included in the EC, together with the EC serial number. These intelligent guesses are computed from information provided externally to the device when it was invoked, and from the internally-held optional values.

• The device builds the EC from the information Alice provided (or accepted from the intelligent guesses) and from the signature blocks of the signed objects. The period of validity of the EC is set to begin at the time taken at the start of the operation (in the first bullet above), and ends one second after the GeneralizedTime recorded at the end of the operation, or, with Alice's approval, a longer period. The device appends Alice's signature to the EC.

THE EMPOWERMENT CERTIFICATE

As an alternative to certificates described in prior art, the described system provides for Alice's software to send Bob an empowerment certificate. This alternative mechanism has a number of unique advantages that mean that Alice does not need to be "issued" with a traditional certificate (or, indeed, any digital certificate at all).

Although Alice has not been "issued" with a certificate, her software still transmits a certificate with every object she signs, but it is always a certificate that her software has built for her and that she herself signs immediately after signing the object to be signed. The whole transaction can sometimes be completely encapsulated in the self-signed certificate alone, making the signing of an associated object unnecessary. The described system calls these special self-signed certificates "empowerment certificates".

Empowerment certificates can be seen as a mechanism by which a user empowers others to gain access to their personal data, including their public key which can be considered to be an ordinary piece of personal data.

The generation of an empowerment certificate includes the following steps. The objects to be signed, if any, are signed first, with a forward reference to the empowerment certificate about to be created included in the data to be signed. The empowerment certificate is then created and signed, with a backward reference to the signature blocks of the signed objects (if any).

The following information is contained in an empowerment certificate:

- .1 A distinguished name that Alice asserts as "issuer".
- .2 The same distinguished name as subject.
- .3 The distinguished name of the relying party.

- 4 The distinguished name of an RA who can resolve Alice's distinguished name to a public key value (or to one or more such values).
 - 5 .5 A period of validity beginning one second before the time taken at the start of the signing operation and ending no earlier than two seconds after that time.
 - .6 (Optionally) a set of attribute definitions.
 - .7 For each attribute definition, either an asserted value or the distinguished name of an RA who holds that attribute value for the subject.
 - 10 .8 (Optionally) the distinguished name of an RA who holds the particular attribute that is the subject's public key value.
 - .9 (If any) the signature block(s) over the previously signed object(s).
 - 15 .10 (If any) a random nonce or other information provided by the relying party. A nonce is typically a large number whose value until it is generated is unpredictable.
 - .11 (Optionally) the subject's public key or one of the subject's public keys, or a reference to such a key.
 - 20 .12 (Optionally) policy information. Alice might include a statement of the purposes for which she agrees that the personal information asserted or referenced in the empowerment certificate may be used, or the purposes for which she states that it may not be used. She may also indicate her approval for the later generation of a custom qualified certificate using the EC.
 - 25 .13 The subject's signature over all the above. There are circumstances (basically, those circumstances in which the signature on the empowerment certificate will never be verified) in which the signature can be omitted, but these circumstances are not discussed further.
 - 30
35
40
- Optionally, the model allows for the possibility that one or more of the RAs which hold the data to be provided are referenced indirectly in the empowerment certificate rather than by distinguished name. The EC might identify a proxy service which knows which RA is to be used for each attribute. There is clearly no limit to the amount of such indirection (one proxy pointing to another proxy, and so on) which might in principle be implemented.

On receiving the empowerment certificate and any signed object(s) from Alice, Bob has four options:

1. Bob may just simply believe what Alice has asserted, not even bothering to check the signature on the empowerment certificate.

At its simplest, the described system acts as a method of transmitting unauthenticated personal data. If Bob is a government agency and Alice wants to be mailed an information leaflet, then it does not much matter if she is lying about her name and home address. This simple use of the empowerment certificate can also deliver the same sort of benefits as browser cookies.

More usually, if there is an accompanying signed object, Bob may not bother to check the signature on the empowerment certificate if he has an longterm custom certificate cached which contains Alice's public key. He will simply pull Alice's distinguished name from the empowerment certificate, find the relevant longterm custom certificate and extract her public key from there to check the signature on the signed object.

2. Alternatively, Bob may check the signature using an asserted value of the public key and just simply believe the rest of the asserted information (if any) if the signature checks out.

This is of some use because, if Bob caches empowerment certificates, it can provide a session mechanism in applications where key revocation is not important. That is, Bob will associate Alice's first visit to his website with her second and subsequent visits, without necessarily getting to know for sure any of Alice's personal data except her public key value. Bob can prevent replay attacks by supplying a nonce for each visit or by checking for increasing empowerment certificate serial numbers. If Alice asserts some other identifier (even a pseudonym) on any visit, then she need not assert her public key on subsequent visits. This mechanism cannot, however, recover from compromise of Alice's signing device, or from Alice rolling over her key. In the first case, someone else can take over the "session"; in the second case the session ends without the possibility of any in-band explanation to Bob.

Despite its limitations, this mechanism has considerable advantages compared to password-based website logon schemes.

3. Another possibility is that Bob checks the signature on the empowerment certificate using a public key value for Alice that he has cached on a longterm custom certificate or knows in some other way (because he is her DRA, for example).

This provides a method of authentication that can cope with revocation.

Once again, Bob can use a nonce or a serial number check to guard against replays. Bob may also be happy to believe without further assurance the asserted information (if any) in the empowerment certificate that differs from what he already has cached or otherwise knew.

5

This use of empowerment certificates provides a method for subjects to inform RAs of changes they need to make to their databases. Archive of the empowerment certificate provides an audit record signed by the subject.

10

4. Most importantly of all, Bob can use the empowerment infrastructure to convert a properly-signed empowerment certificate into a custom certificate (or, indeed, more than one custom certificate). This is a crucial part of the described system and is explained next. If Bob takes this route, it is prudent for him to check that Alice has correctly copied the object signature block (if any) to the empowerment certificate.

15

THE CUSTOM CERTIFICATE

20

Just as Alice has a contract with one or more RAs, so Bob, if he wants to convert an empowerment certificate into a custom certificate, needs to have a contract with one or more CAs. The process is straightforward. At any time before the expiry of the empowerment certificate (or as soon as possible after the expiry of an instantaneous empowerment certificate), and as many times as he likes, Bob sends to a CA an empowerment certificate which he has received and the CA signs and returns an equivalent custom certificate, customised to Bob's requirements. There are no restrictions in the system on Bob's choice of CA, or on how many times (provided, in the case of an instantaneous empowerment certificate that he is quick), or to how many different CAs he sends the same empowerment certificate.

25

30

What the CA is doing is executing Alice's mandate, given when she created the empowerment certificate, for certain of her personal data to be shared with Bob. Her public key a piece of personal data which may be shared in this way.

35

The following describes the method steps. If anything goes wrong, the process ends and Bob's request is rejected with a reason code.

40

The CA generates the serial number of the custom certificate being prepared and copies the empowerment certificate serial number, the hash of the empowerment certificate, the object signature blocks (if any) and the nonce (if any) as attributes in the custom certificate. The CA copies its own distinguished name into the issuer field along with a timestamp

For a longterm empowerment certificate, the CA checks that the period of validity of the empowerment certificate will not have expired before the time likely to assemble and sign a custom certificate. For an instantaneous empowerment certificate, the CA checks that only a reasonable period of time has passed since the empowerment certificate was signed. "Reasonable" means that Alice's personal data is highly unlikely to have changed since she signed the empowerment certificate.

For both longterm empowerment certificates and instantaneous empowerment certificates (for which the reasonable period has not passed), the CA will set the validity period start time of the custom certificate the same as the start time of the empowerment certificate. Otherwise (and this will clearly apply to longterm custom certificates only), the validity period start time will be set to the time by the CAs clock. As an option, to support store-and-forward transactions, it may be useful for the start time to be set to a significantly earlier time.

The custom certificate validity period end time will be set to the empowerment certificate validity period end time, or to an earlier time that Bob specifies.

The CA checks that Bob is named as relying party in the empowerment certificate and names Bob as the relying party in the custom certificate. Within defined rules, certain changes to the presentation of Bob's name is permitted. (The analogy here is the flexibility with which banks match payee names on cheques to accountholder names.)

The CA checks that the empowerment certificates subject name and "issuer" name are identical and copies the value into the subject field of the custom certificate. Again, within defined rules, changes to Alice's name are permitted.

The CA ignores (that is, treats as if they were not present) any attribute in the empowerment certificate that has been asserted rather than referenced to an RA. Asserted attribute values in empowerment certificates have benefit in the part of the communication between Alice and Bob not involving a CA. Asserted public key values do have one use within the infrastructure, which is explained below.

The CA then presents the empowerment certificate to the RA identified in the empowerment certificate as able to resolve Alice's distinguished name into her public key. If this is a longterm empowerment certificate, the RA will first check to see if Alice has revoked it. How the RA does that is explained later. (The instantaneous or longterm status of the custom

certificate is irrelevant.) In any case, the RA checks the validity period of the empowerment certificate.

5 The RA consults its database, extracts the value of the public key and checks the empowerment certificate. If it knows of more than one public key for Alice it will try each in turn, guided by hints she has included in the empowerment certificate (for example, asserting the value of, or the value of the hash of, a public key), until the signature on the empowerment certificate checks out.

10 For a longterm custom certificates only, the RA adds, to each of the attributes that compose the distinguished name, a label of the following form ("DN flag", CA's distinguished name, custom certificate serial number, expiry date). No label is added for an instantaneous custom certificate.

15 (The instantaneous or longterm status of the empowerment certificate is irrelevant for this decision.)

20 The RA examines the empowerment certificate to see if it is named as the RA for any of the predicate attributes, including the public key. It pulls out of its database any values that Alice has empowered. For a longterm custom certificate only, the RA adds to each attribute a label of the form ("att flag", CA's distinguished name, custom certificate serial number, expiry date). No label is added for an instantaneous custom certificate. (The instantaneous or longterm status of the empowerment certificate is irrelevant for this decision.)

25 For longterm custom certificates, the RA caches the empowerment certificate, and records the mapping of empowerment certificate and custom certificate serial numbers, expiry dates and "issuers".

30 The RA sends the following information back to the CA:

·14 Alice's public key value.

·15 The values of any predicate attributes for which it is responsible.

35 If a public key value is included among the predicate attributes and Alice has more than one public key, the RA will choose one on the basis of the public key value or hash value that Alice asserted. This may or may not be the same value as the public key value returned above, because Alice might approve with a signature using one private key the creation of a custom certificate containing the public key corresponding to another of her private keys.

40

The CA is now able to check the signature on the empowerment certificate, and does so. If there are any more RAs to be consulted, the CA sends out the empowerment certificate in parallel to them, along with the first public key value returned by the first RA. The RAs check the empowerment certificate, including again its expiry and revocation status, use the distinguished name in the empowerment certificate, or the public key value, to identify the subject, and return the values. As before, for longterm custom certificates they label "att flag" attributes, cache the empowerment certificate and map the empowerment certificate to the custom certificate.

Note that the public key to be included in a public key custom certificate may be provided by an RA other than the RA who initially resolved Alice's distinguished name into her public key.

With all the attribute information back, the CA now marks the certificate to indicate the certificate policy that Bob has requested. In particular, if Bob has asked for a qualified certificate, and the CA is happy that this is possible, the CA marks the certificate as qualified, with a liability limitation the lower of what Bob has requested and what the CA is willing to offer. The policy Alice set in the EC will also constrain whether or not a custom qualified certificate can be generated.

To get the policy and liability he wants, Bob can even submit the empowerment certificate independently to two or more CAs, or to the same CA multiple times, playing off the weakness in one policy with the strength of another, to use one custom certificate to reinforce another, or to spread a qualified certificate liability over two or more CAs.

There is one important constraint on the policy that the CA defines in the custom certificate. Any personal data policy limitations that Alice defined in the original empowerment certificate are carried forward into the custom certificate.

Finally, the CA informs the RA who resolved Alice's distinguished name into her public key the fact of transfer to Bob of the custom certificate. The CA will provide the serial numbers of the empowerment certificate and longterm custom certificate, and say whether the longterm custom certificate is qualified or not (so that Alice knows if her signature was upgraded to qualified status as defined in article 5.1 of the EU Electronic Signatures Directive). The RA is specifically not told anything else about the policy, and is not told the amount of any liability limitation. (It is none of Alice's business what value Bob attaches to his relationship with her.)

Bob obviously has an option to ask for only a subset of the possible predicate attributes to be included.

5 Figure 6 shows a flow diagram of the method 600 carried out by the CA. The method 600 starts with the empowerment certificate being sent by Bob to the CA 601. At step 602, the CA generates a serial number for the new custom certificate, checks that the data of the empowerment certificate is consistent and copies the data into the custom certificate and enters its name as the issuer of the custom certificate. If any data is inconsistent
10 603, the empowerment certificate is rejected and returned to Bob 604.

The CA checks the validity of the empowerment certificate by first ascertaining if the certificate is instantaneous or longterm 605. If the empowerment certificate is instantaneous, the time since it was generated
15 is checked to make sure this is within a predetermined time 606. If the empowerment certificate is longterm, the validity period is checked 607. If the empowerment certificate is outside its validity period, the empowerment certificate is rejected and returned to Bob 604.

The CA then sets the validity period of the custom certificate 608 and
20 sends the custom certificate to the RA 609. The RA processes the custom certificate and sends Alice's public key to the CA 610. The CA checks the signature of the empowerment certificate with the public key 611. If some of the data referred to in the empowerment certificate is held in other RAs the CA will send requests to the other RAs for the data. The CA signs the
25 custom certificate and transmits it to Bob 612. The CA also informs the RA that the data has been sent to Bob.

THE CUSTOM CERTIFICATE REVOCATION LIST

30 Just as the system provides for custom certificates, so too there are custom certificate revocation lists. They apply to longterm custom certificates only, because instantaneous custom certificates expire within a second of their generation, so the question of their revocation never arises.

35 Through a mechanism that is about to be explained, a CA will become aware of any change to information included in a longterm custom certificate that it has signed, provided that the change occurs before the expiry of the longterm custom certificate concerned. Also, Alice can at any time revoke
40 any of the empowerment certificates she has signed, which means that the corresponding longterm custom certificates must also be revoked. Bob can also ask for any longterm custom certificate in which he is named as relying party to be revoked.

A CA maintains a separate custom certificate revocation list (CRL) for each of its customers, and each customer only gets to see its own CRL. Bob can consult his CRL anytime he wishes, can specify the normal frequency he wants CRLs updated, and can even force the creation of a new CRL at any time. Bob can also be asked to be notified each time a new CRL is available for his inspection. Bob can archive CRLs so that he can later prove that a particular longterm custom certificate was unrevoked at any particular time.

Whenever a certificate serial number appears in a CRL, Bob will want to archive the revoked certificate. If the empowerment certificate that matched the revoked longterm custom certificate is still unexpired, then Bob can resubmit the matching empowerment certificate and try to get a new longterm custom certificate with updated content. Whether he is successful or not depends on the reason for revocation, and Bob can see the revocation reason code in his CRL.

Clearly, if Alice revoked the empowerment certificate, then no way is the infrastructure going to yield up a longterm custom certificate to Bob. Alice has withdrawn that particular empowerment to her personal data. And a longterm custom certificate will not be recoverable if Alice's distinguished name is deleted.

If only the value of an attribute or a public key has changed, or if Alice has simply changed the way her personal data is allocated to RAs, then the empowerment certificate can usually be resubmitted and a replacement longterm custom certificate obtained, valid for the remaining duration of the empowerment certificate.

Bob can request a longterm custom certificate at any time before the empowerment certificate expiry. Bob can even contract with the CA for the CA to automatically process a new request every time a revocation occurs, without Bob needing to start the exercise off. And Bob can present the same empowerment certificate to different CAs during its lifetime.

So, as Alice rolls over her key pair, or changes her name on marriage, or receives an increased purchasing limit from Acme, or changes bank, or moves house, or changes phone number, or even changes employer, the longterm custom certificates around the world which name her as subject will quickly get revoked and replaced. Bob's address book will always be up to date. Alice needs to tell just one of her RAs of her change of circumstances, and everyone she has empowered to know about those circumstances will very soon know what has happened. This applies to every piece of data in unexpired

longterm custom certificates - identifiers, predicate, authenticators, authorisers, locators.

Every time a CA revokes a longterm custom certificate it flags the serial number of the revoked longterm custom certificate to the RA who resolved Alice's distinguished name into her public key.

The following describes how the method works in detail.

Alice is optionally able to maintain, through her software functionality, constructs known as empowerment certificate revocation lists (ECRLs). At any time she can present to any of her RAs an ECRL listing the serial numbers of previously-generated longterm empowerment certificates still valid that she wishes to revoke. (Instantaneous empowerment certificates expire shortly after their creation, so the question of their revocation never arises.)

When any of the RAs receives an ECRL, it extracts from the list the serial numbers of all the empowerment certificates which it has processed for Alice, looks at its mapping table to find the matching CA names and custom certificate serial numbers, and sends signed messages to each CA instructing revocation on the grounds of "empowerment certificate revocation".

If a particular empowerment certificate names more than one RA, Alice can send the ECRL to any one of them. This provides her with the ability to revoke a part of an empowerment certificate, at the granularity of the RA. It is even possible to allow revocation at the granularity of an attribute. There is a requirement for a revocation code "partial empowerment certificate revocation".

- If Alice decides to move an item of her personal data from one RA to another, the RA will look at the labels on that item of data, extract the serial numbers of unexpired custom certificates and send signed revocation messages to the relevant CAs, with a reason code "change of RA".
- Every time a piece of Alice's data changes value in its database, the RA will examine the labels attached and will send out signed revocation messages for each custom certificate. For custom certificates where the DN flag is set, the revocation reason will be "identity deleted". Where the att flag is set, the reason will be "attribute change".

- Finally, if, through methods not defined in the system, an RA learns of the death of a subject, it will cause the revocation of all that subject's unexpired custom certificates with a reason code "death of subject".

5

It is worthwhile resubmitting unexpired empowerment certificates only if the revocation reason was "partial empowerment certificate revocation", "change of RA" or "attribute change".

10

Figure 7 shows the diagram of Figure 3 with the addition of the certificate revocation lists. An empowerment certificate revocation list 701 is transmitted by Alice 302 to the RA 306. The RA 306 has a mapping table 702 in which a record of all empowerment certificates and custom certificates is kept with reference to their serial numbers and a record of the CAs to which the data has been supplied. The RA 306 can inform the CAs of any custom certificates which should be revoked further to a revocation request from Alice 302. The CA 310 keeps a certificate revocation list 703 for each relying entity such as Bob 304.

15

20

THE INFRASTRUCTURE

25

The empowerment infrastructure consists of a secure (that is, signed and encrypted) messaging and transaction system linking a set of RAs and CAs which offer empowerment services to their customers. Methods of implementing such transaction systems are well described in prior art.

30

As the CAs and RAs communicate securely among themselves, they in turn could exploit the same mechanisms as we have shown Alice and Bob to exploit.

35

Improvements and modifications can be made to the foregoing without departing from the scope of the present invention.

CLAIMS

- 5 1. A method for supply of data relating to a described entity (302) to a
relying entity (304) comprising:
generating a first digital certificate signed with an electronic signature
by a first signing entity and including:
- 10 *one or more* (one or more attributes of the described entity (302));
one or more attributes of the first digital certificate which include
one or more attributes identifying the first signing entity;
an indication of data relating to the described entity (302) which is
to be supplied;
an indication of one or more sources (306, 500) for the data to be
15 supplied; and
one or more attributes identifying one or more relying entities (304)
to which the data is to be supplied;
- that be* the relying entity (304) forwarding the first digital certificate for
signature processing;
- 20 a source (306, 500) supplying the data indicated in the first digital
certificate.
2. A method as claimed in claim 1, wherein a source (306, 500) can hold
data or can refer to one or more further sources (306, 500).
- 25 3. A method as claimed in claim 1 or claim 2, wherein the first signing
entity is the described entity (302).
4. A method as claimed in any one of claims 1 to 3, wherein the first
30 digital certificate includes a reference, nonce or other data which the
relying entity (304) has previously requested to be included.
5. A method as claimed in any one of claims 1 to 4, wherein some or all
of the data relating to the described entity (302) is supplied by means of
35 a second digital certificate to the relying entity (304), the second
digital certificate signed with an electronic signature by a second signing
entity and including:
- one or more attributes of the described entity (302) including the
data which is to be supplied;
- 40 one or more attributes of the second digital certificate which
include one or more attributes identifying the second signing entity;
and
one or more attributes identifying one or more relying entities (304)
to which the data is to be supplied.
- 45

6. A method as claimed in claim 5, wherein the first digital certificate authorises the relying entity (304) to use the first digital certificate to obtain a second digital certificate.

5 7. A method as claimed in claim 6, wherein the relying entity (304) is authorised to obtain a second digital certificate which is marked as qualified.

10 8. A method as claimed in any one of claims 5 to 7, wherein the second digital certificate includes one or more attributes of the first digital certificate.

15 9. A method as claimed in any one of claims 5 to 8, wherein at least some of the contents of the first digital certificate is copied to the second digital certificate.

20 10. A method as claimed in any one of the preceding claims, wherein the method includes the relying entity (304) forwarding the first digital certificate to an intermediate entity (308) to obtain data from a source (306, 500).

11. A method as claimed in claim 10, wherein the intermediate entity (308) generates the second digital certificate.

25 12. A method as claimed in any one of claims 5 to 11, wherein the second digital certificate includes one or more attributes identifying the relying entity (304) which are different from the one or more attributes identifying the relying entity (304) included in the first digital certificate.

30 13. A method as claimed in any one of claims 5 to 12, wherein the second digital certificate includes one or more attributes identifying the described entity (302) which are different from one or more attributes identifying the described entity (302) included in the first digital certificate.

35 14. A method as claimed in any one of the preceding claims, wherein the described entity (302) generates a digital signature using a private key with a corresponding public key and the first signing entity includes the digital signature or a cryptographic digest thereof in the first digital certificate, and the data to be supplied to the relying entity (304) includes the public key.

15. A method as claimed in any one of the preceding claims, wherein the first digital certificate includes a period of validity.

5 16. A method as claimed in any one of claims 5 to 15, wherein the second digital certificate includes a period of validity.

10 17. A method as claimed in claim 15 or claim 16, wherein the period of validity of the first digital certificate or the second digital certificate is that short period of time during which a digital signature was generated.

15 18. A method as claimed in any one of the preceding claims, wherein the data indicated in the first digital certificate includes confirmation of a payment or debt due from the described entity (302) identified in the first digital certificate to the relying entity (304) identified in the first digital certificate.

20 19. A method as claimed in claim 18, wherein a second signing entity indicates in a second digital certificate a guarantee of a debt indicated as due in a first digital certificate.

25 20. A method as claimed in claims 5 to 19, wherein a change in previously supplied data is indicated by the supply of a list identifying a second digital certificate relating to the previously supplied data.

30 21. A method as claimed in any one of the preceding claims, wherein a list (701, 703) identifies a first or second digital certificate specifying data which is no longer authorised to be supplied to the relying entity (304).

35 22. A method as claimed in claim 20 or claim 21, wherein the generation of the list (701, 703) includes one or more attributes identifying the relying entities (304) to which the list (701, 703) relates.

40 23. A method as claimed in any one of claims 5 to 22, which includes generating and storing a list (703) for the second digital certificates, which is indexed by one or more attributes identifying relying entities (304) such that all second digital certificates in the list (703) relevant to a relying entity (304) can be identified.

24. A system for supply of data relating to a described entity (302) to a relying entity (304), the system comprising:

a first signing entity application, a relying entity application and a data store (504) wherein the data store (504) holds data relating to the described entity (302);

the first signing entity application has means for generating a first digital certificate signed with an electronic signature by the first signing entity application and including:

one or more attributes of the described entity (302);

one or more attributes of the first digital certificate which include one or more attributes identifying the first signing entity;

an indication of data relating to the described entity (302) which is to be supplied;

an indication of one or more sources (306, 500) for the data to be supplied; and

one or more attributes identifying one or more relying entities (304) to which the data is to be supplied;

the relying entity application has means for forwarding the first digital certificate for processing; and

means for supplying the data indicated in the first digital certificate from the data store (504).

25. A system as claimed in claim 24, wherein a source (306, 500) holds the data store (504) or can refer to one or more further sources (306, 500).

26. A system as claimed in claim 24 or claim 25, wherein the first signing entity is the described entity (302).

27. A system as claimed in any one of claims 24 to 26, wherein the first digital certificate includes a reference, nonce or other data which the relying entity (304) has previously requested to be included.

28. A system as claimed in any one of claims 24 to 27, wherein a second digital certificate is provided for supplying the data relating to the described entity (302) to the relying entity application, the second digital certificate signed with an electronic signature by a second signing entity application and including:

one or more attributes of the described entity (302) including the data which is to be supplied;

one or more attributes of the second digital certificate which include one or more attributes identifying the second signing entity; and

one or more attributes identifying one or more relying entities (304) to which the data is to be supplied.

29. A system as claimed in any one of claims 24 to 28, wherein the system includes an intermediate entity application to which the relying entity application forwards the first digital certificate to obtain data from the data store (504).

5

30. A system as claimed in any one of claims 24 to 29, wherein the system includes more than one data store (504) holding data relating to the described entity (302).

10

31. A system as claimed in any one of claims 24 to 30, wherein a data store (504) has a means of determining for an item of data included in the data store (504) information concerning or contained in a first digital certificate which has referenced that item

15

32. A system as claimed in any one of claims 28 to 31, wherein a data store (504) has a means of determining for an item of data included in the data store (504) information concerning or contained in a second digital certificate which provides the value of that item.

20

33. A system as claimed in any one of claims 29 to 32, wherein the intermediate entity application has a storage means for storing second digital certificates referenced by the relying entities (304) identified in the second digital certificates.

25

34. A system as claimed in any one of claims 24 to 33, wherein the system includes a proxy entity application to which the relying entity application or the intermediate entity application forwards the first digital certificate to obtain information specifying to which data store (504) or other proxy entity application the first certificate should next be forwarded

30

35. A computer program product stored on a computer readable storage medium, comprising computer readable program code means for performing the steps of:

35

generating a digital certificate signed with an electronic signature by a signing entity and including:

one or more attributes of a described entity (302);

one or more attributes of the digital certificate which include one or more attributes identifying the signing entity;

40

either an indication of data relating to the described entity (302) which is to be supplied and an indication of one or more sources (306, 500) or the data itself; and

one or more attributes identifying one or more relying entities (304) to which the data is to be supplied.

36 A digital certificate signed with an electronic signature by a signing entity and comprising:

one or more attributes of a described entity (302);

5 one or more attributes of the digital certificate which include one or more attributes identifying the signing entity;

either an indication of data relating to the described entity (302) which is to be supplied and an indication of one or more sources (306, 500) or the data itself; and

10 one or more attributes identifying one or more relying entities (304), wherein the relying entities (304) are entities to which the data relating to the described entity (302) is to be supplied.

37. A method of providing a digital signature based on a digital certificate comprising:

15 generating a digital signature using a private key corresponding to a public key, the signed data including:

one or more attributes identifying a digital certificate to be generated;

20 generating a digital certificate signed with an electronic signature by a signing entity and including:

one or more attributes of a described entity (302) which are sufficient to obtain the public key;

25 one or more attributes of the digital certificate which include one or more attributes identifying the signing entity; and

an indicated period of validity of the digital certificate which begins earlier than the time of generation of the digital certificate;

wherein the digital certificate is generated after the generation of the digital signature.

38. A method as claimed in claim 37, wherein more than one digital signature can be generated which identifies the same digital certificate.

35 39. A method as claimed in claim 37 or claim 38, wherein the period of validity of the digital certificate is that short period in which the digital signature was generated.

40 40. A method as claimed in any one of claims 37 to 39, wherein the one or more attributes identifying the digital certificate to be generated given in the digital signature include a serial number.

41. A method as claimed in claim 40, wherein the lowest available serial number which can be used for the next digital certificate to be generated or the last used serial number using each private key is recorded.

42. A system for providing a digital signature based on a digital certificate, the system comprising:
 a described entity application with means for generating a digital signature using a private key corresponding to a public key, the signed data including:

one or more attributes identifying a digital certificate to be generated;

a signing entity application having means for generating a digital certificate with an electronic signature and including:

one or more attributes of a described entity (302) which are sufficient to obtain the public key;

one or more attributes of the digital certificate which include one or more attributes identifying the signing entity; and

an indicated period of validity of the digital certificate which begins earlier than the time of generation of the digital certificate;

wherein the digital certificate is generated after the generation of the digital signature.

43. A computer program product stored on a computer readable storage medium, comprising computer readable program code means for performing the steps of:

generating a digital signature using a private key corresponding to a public key, the signed data including:

one or more attributes identifying a digital certificate to be generated;

generating a digital certificate signed with an electronic signature by a signing entity and including:

one or more attributes of a described entity (302) which are sufficient to obtain the public key;

one or more attributes of the digital certificate which include one or more attributes identifying the signing entity; and

an indicated period of validity of the digital certificate which begins earlier than the time of generation of the digital certificate;

wherein the digital certificate is generated after the generation of the digital signature.

44. A digital certificate signed with an electronic signature by a signing entity and comprising:

one or more attributes of a described entity (302);

one or more attributes of the digital certificate which include one or more attributes identifying the signing entity;

an indicated period of validity of the digital certificate which begins earlier than the time of generation of the digital certificate.

5

45. A digital certificate as claimed in claim 44, wherein the indicated period of validity of the digital certificate ends no later than the time of generation of the digital certificate.

10

46. A digital certificate as claimed in claim 44 or claim 45, wherein the described entity (302) is the signing entity.

47. A digital certificate as claimed in any one of claims 44 to 46, wherein the digital certificate includes a time stamp indicating the time of generation.

15

48. A digital signature using a private key corresponding to the public key derivable from a digital certificate as claimed in claim 44, wherein the digital certificate is generated after the generation of the digital signature,

the signed data including:

20

one or more attributes identifying the digital certificate to be generated.

25



INVESTOR IN PEOPLE

Application No: GB 0126596.6
Claims searched: 1-36

Examiner: John Cullen
Date of search: 4 October 2002

Patents Act 1977 Search Report under Section 17

Databases searched:

<p>UK Patent Office collections, including GB, EP, WO & US patent specifications, in:</p> <p>UK CI (Ed.T): H4P (PDCSA)</p> <p>Int CI (Ed.7): G06F 1/00; H04L 9/32, 29/06</p> <p>Other: Online: WPI, EPODOC, JAPIO</p>

Documents considered to be relevant:

Category	Identity of document and relevant passage	Relevant to claims
A, E	WO 2001/089133 (SURETY.COM) See Fig. 1 A2	---
A	US 6310966 B1 (GTE SERVICE) See Figs. 1 and 2.	---
A	JP 2001-092354 (NIPPON TELEGRAPH) 6.4.2001 (See PAJ Abstract and WPI Abstract Accession No. 2002-085134/12).	---
A	X.509 Certificates and Revocation Lists (CRLs), Sun Microsystems, 20.05.1998, http://java.sun.com/products/jdk/1.2/docs/guide/security/cert3.html . See section entitled 'What's Inside an X.509 Certificate?'.	---

X	Document indicating lack of novelty or inventive step	A	Document indicating technological background and/or state of the art.
Y	Document indicating lack of inventive step if combined with one or more other documents of same category.	P	Document published on or after the declared priority date but before the filing date of this invention.
&	Member of the same patent family	E	Patent document published on or after, but with priority date earlier than, the filing date of this application.

(19)



Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 1 081 632 A1

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:
07.03.2001 Bulletin 2001/10

(51) Int Cl.7: **G06K 9/68**

(21) Application number: **99870178.3**

(22) Date of filing: **01.09.1999**

(84) Designated Contracting States:
**AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE**
Designated Extension States:
AL LT LV MK RO SI

(72) Inventor: **KEYWARE TECHNOLOGIES,
c/o Declercq Francis
B-1930 Zaventem (BE)**

(71) Applicant: **Keyware Technologies
8900 Ieper (BE)**

(74) Representative: **Quintelier, Claude et al
Gevers & Vander Haeghen,
Patent Attorneys,
Rue de Livourne 7
1060 Brussels (BE)**

(54) **Biometric authentication device**

(57) A biometric authentication device provided for managing access to at least one entity, said device being connectable to a database storing biometric templates, said device comprising a set of bio-engines and a data capture unit provided to collect life biometric data, each of said bio-engines being provided for performing a dedicated biometric authentication operation with said biometric templates and said life biometric data and for generating a score as a result of said authentication operation, said device comprises a decision unit operating according to a master-slave relationship, wherein said

decision unit being the master, said decision unit being provided for receiving each of said scores and for assigning a respective weight factor to each of said scores and forming a set of weighted scores therewith, said decision unit being further provided for combining said weighted scores and generating a verified score therewith, said decision unit being also provided for comparing said verified score with a threshold value and for generating an access enable signal as a result of a positive comparison and an access refusal signal as a result of a negative comparison.

EP 1 081 632 A1

Description

[0001] The present invention relates to a biometric authentication device provided for managing access to at least one entity, said device being operatively connectable to a database provided for storing biometric templates, said device comprising a set of bio-engines each having an input for receiving said biometric templates and life biometric data originating from a data capture unit provided to collect life data, each of said bio-engines being provided for performing a dedicated biometric authentication operation with said biometric templates and said life biometric data and for generating a score as a result of said authentication operation.

[0002] Biometric authentication devices are known and their use is for example described in the article "Person authentication by fusing face and speech information" written by B. Duc, G. Maître, S. Fischer and J. Bigün and presented on the First International Conference AVBPA in Crans-Montana in March 1997 (p. 311-318). Biometrics is a science of measuring unique physical or behavioural characteristics such as the pattern of the voice of a person, or the micro-visual pattern of his retina, the tiny swirls etched in the skin of his fingertip, this facial appearance etc. Biometric authentication is used to manage access to an entity such as for example an office or a room, a bank account, a computer or a network, etc. The biometric data of one or more persons is stored in a database to which the bio-engines performing the biometric authentication have access. Data capture units such as for example a camera, a fingerprint scanner or a microphone collect the life biometric data from the person who want to get access to the entity protected by the biometric authentication device. The bio-engines perform than authentications and issue a score. If the score is above the predetermined threshold the person will get access to the entity. If the score is below the threshold access will be refused. The bio-engines are provided for a dedicated biometric authentication, i.e. there is a bio-engine for voice authentication, one for the fingerprint, another for the facial appearance etc. Each bio-engine generates its own score independent of the other engines.

[0003] Operating with a single bio-engine has a major drawback because the life biometric data of the person such as collected by the data capture unit can change. So for example a person having a cold will have his voice sound differently such that the bio-engine performing the voice authentication will issue a lower score which could lead to an access refusal. This could be solved by lowering the threshold. However lowering the threshold leads to an increase of false acceptance which for certain secure applications is unacceptable. Therefor attempts have been made to combine the outputs of several bio-engines such as described in the referred article.

[0004] A drawback of the known devices where the output of several biometric engines are combined is that

they do not enable a true combination of the scores as each bio-engine continues to operate on its own by generating its own decision based on its internal score.

[0005] It is an object of the invention to realise a biometric authentication device enabling a true combination of the scores of the different bio-engines.

[0006] A biometric authentication device according to the present invention is therefor characterized in that said device comprises a decision unit connected to said bio-engines and operating according to a master-slave relationship, wherein said decision unit being the master, said decision unit being provided for receiving each of said scores and for assigning a respective weight factor to each of said scores and forming a set of weighted scores therewith, said decision unit being further provided for combining said weighted scores and generating a verified score therewith, said decision unit being also provided for comparing said verified score with a threshold value and for generating an access enable signal as a result of a positive comparison and an access refusal signal as a result of a negative comparison. The master-slave governing the relationship between the decision unit and the bio-engines enables such a true combination as the bio-engines scores are weighted by the decision unit. If one score is for example below the threshold whereas the others are above their respective thresholds, the decision unit can reduce the impact of such a bio-engine by assigning a low weight factor. As the decision unit has the scores of the different bio-engines a relative weighing of the different scores becomes possible. The decision to enable or not access to the entity is thus no longer based on a combination of the individual outputs of the different bio-engines, but on a combination of the scores realised by the decision unit.

[0007] A first preferred embodiment of a biometric authentication device according to the invention is characterized in that the decision unit is connected with a first bio-decision engine which is provided for executing a serial combinatorial operation with the scores generated by at least one of said bio-engines, said first bio-decision engine being provided to operate as a slave from said decision unit. This enables to have each individual bio-engine performing several authentication operations and to serially combine the scores issued by a same bio-engine.

[0008] A second preferred embodiment of a biometric authentication device according to the invention is characterized in that the decision unit is connected with a second bio-decision engine, which is provided for executing a parallel combinatorial operation with the scores generated by at least one of said bio-engines, said second bio-decision engine being provided to operate as a slave from said decision unit. This enables to have each individual bio-engine performing several authentication operations and to combine in parallel the scores issued by a same bio-engine.

[0009] A third preferred embodiment of a biometric

authentication device according to the invention is characterized in that said decision unit is provided for generating a control signal when said verified score is below said threshold, said decision unit being further provided for determining a set of further weight factors under control of said control signal and assigning them to said scores and generating a further verified score therewith. This enables to reconsider the authentication operation if one of the scores was insufficient for example due to particular circumstances such a user having a bad voice quality due to a cold.

[0010] A fourth preferred embodiment of a biometric authentication device according to the invention is characterized in that said further weight factors and said weight factors each time satisfy a predetermined relationship. The weight factors are thus normalized which facilitates the calculation and keeps the verified score reliable.

[0011] Preferably said decision unit comprises a core server which is provided for generating said verified score and executing said comparison. This facilitates the architectural structure of the device.

[0012] Preferably characterized in that said decision unit comprises a module manager which is provided for managing data traffic between said bio-engines and said core server. An improved architecture for the data traffic is thus obtained.

[0013] Preferably said data capture unit is connected to an interface to which a feature module is connected, said feature module being provided for input of client dedicated features. The end user can in such a manner supply his own particular features to the device, such as for example those relating to a particular group of users or relating to particularities of individual users.

[0014] A fifth preferred embodiment of a biometric authentication device according to the invention is characterized in that said biometric templates are stored in a memory formed by either a smartcard, a harddisk, a EEPROM or a flash memory. In particular when a smartcard is used, the biometric templates of the owner are stored thereon and there is no need to let them travel over a publicly accessible network.

[0015] A sixth preferred embodiment of a biometric authentication device according to the invention is characterized in that said decision unit is connected to a self learning module which is provided for substituting into said database a biometric template by a life biometric data under control of a second control signal generated by said decision unit upon detection of a score issued by a bio-engine which is higher than a further predetermined threshold value. This enables to up-date the biometric templates and thus to improve the reliability of the access monitoring.

[0016] A seventh preferred embodiment of a biometric authentication device according to the invention is characterized in that said decision unit is connected to an environmental module which is provided for generating a trigger signal, said decision unit being provided

to modify the weight factors under control of said trigger signal. This enables to take into account environmental conditions such as background noise or high or pour light intensity.

[0017] The invention will now be described in more details by means of the drawings showing a preferred embodiment of a device according to the invention. In the drawings :

Figure 1 illustrates the relation between a False Accept Rate and a False Reject Rate;

Figure 2 illustrates serial operating bio-engines;

Figure 3 illustrates parallel operating bio-engines;

Figure 4 illustrates a combination of parallel and serial operating bio-engines;

Figure 5 illustrates a set-up of different bio-engines according to the state of the art;

Figure 6 illustrates the principle of a threshold in a bio-engine;

Figure 7 illustrates schematically a set-up of a biometric authentication device according to the present invention;

Figure 8 illustrates the architecture of a biometric authentication device according to the present invention; and

Figure 9 illustrates schematically the operation of a biometric authentication device according to the present invention.

[0018] In the drawings a same reference sign has been assigned to a same or analogous element.

[0019] In biometrics a distinction is made between a "client", who should be recognised as somebody having access to the protected entity and an "impostor" who is someone pretending to be someone else and who should not have access. The protected entity can be a room, an office, a bank account, a computer system, a network etc.

[0020] The False Acceptance Rate (FAR) gives the percentage of falsely accepted impostors

$$FAR = \frac{\text{total number of falsely accepted impostors}}{\text{total number of impostors tested}}$$

[0021] The False Rejection Rate (FRR) gives the percentage of falsely rejected clients.

$$FRR = \frac{\text{total number of falsely rejected clients}}{\text{total number of clients tested}}$$

[0022] The Equal Error Rate (EER) is the percentage corresponding to the threshold level for which the FAR and FRR are equal. Figure 1 illustrates the relation between FAR and FRR. FAR and FRR are inversely proportional as illustrated. The technology tries to lower the EER which is the cross point between the FAR - FRR curve and the curve $y = x$. To lower the EER it is necessary to lower the values of FAR and FRR This can be

obtained by increasing the number of biometric authentications.

[0023] Authentication signifies the general process of verifying the identity claimed by the user. Authentication thus covers as well a authentication process, which is a one to one process, as an identification process, which is a one to many process. Identification answers the question "Who is trying to get in ?", whereas authentication answers the question "Is that really Mr. Jones trying to get in ?" Biometric authentication is used as a general term for a process of checking ones identity by biometric technology.

[0024] A first possibility for increasing the number of biometric authentications is to serially combine the biometric authentication operations such as illustrated in figure 2. Suppose that two biometric authentication operations are performed, one by bio-engine A which performs a voice authentication and one by bio-engine B which performs face authentication. The serial combination starts with the first bio-engine generating a score Sva.

[0025] Due to the serial arrangement the second bio-engine B can only generate a score Svb if the first bio-engine has generated a positive score, i.e. if the first authentication was successful. The FAR_S of the whole system is determined by :

$$FAR_S = FAR_A \times FAR_B$$

The FRR_S of the system is determined by

$$FRR_S = FRR_A + (1 - FRR_A) \times FRR_B$$

By way of example suppose now

$$EER_A = 5 \% \text{ and } EER_B = 2 \%$$

Suppose also that both bio-engines will operate at a threshold where the EER is obtained. The threshold being the value of the score such as generated by the bio-engine at which a positive result i.e. access enabled, is generated. So FAR_A = FRR_A = 5 % and FAR_B = FRR_B = 2%. The serial system will then have the following values :

$$FAR_S = 0.05 \times 0.02 = 0.001 \text{ or } 0.1 \%$$

$$FRR_S = 0.05 + (1 - 0.05) \times 0.02 = 0.069 \text{ or } 6.9 \%$$

Thus the serial combination offers a better FAR_S than each individual system but the FRR_S has become worse. So with a serial combination it is harder to get falsely accepted because one has to pass two or more

authentications, but the probability of being falsely refused has substantially increased.

[0026] A second possibility for increasing the number of biometric authentications is to combine the biometric operations in parallel as illustrated in figure 3. In such a configuration the user has two attempts which are performed independently from each other. The acceptance of a user by one of the engines will not reroute the authentication procedure to the other. If a person is not accepted by one of the engines he could still be accepted by the other. Combining both systems will provide an overall performance with :

$$FAR_S = FAR_A + FAR_B - FAR_A \times FAR_B$$

$$FRR_S = FRR_A \times FRR_B$$

Going back to the example with FAR_A = FRR_A = 5 % and FAR_B = FRR_B = 2 % the following results are obtained :

$$FAR_S = 0.05 + 0.02 - 0.05 \times 0.02 =$$

$$0.07 - 0.001 = 0.069 \text{ or } 6.9 \%$$

$$FRR_S = 0.05 \times 0.02 = 0.001 \text{ or } 0.1 \%$$

Thus a parallel combinatorial system has a better FRR_S than each of the individual system, but the FAR_S has substantially increased.

[0027] A third possibility for increasing the number of biometric authentications is to form a combination of both parallel and serial combinations such as for example illustrated in figure 4. Each of the bio-engines performs in parallel several authentication processes and the output of the first layer of bio-engines (1) (for example the voice authentication) is serially combined to the second layer of bio-engines (2) (for example a fingerprint authentication). With such a set-up a user has three attempts with the first layer and if he is successful in one of those attempts he has again three attempts with the second layer. The overall performance of this system is now :

$$FAR_{S1} = FAR_{1a} + (1 - FAR_{1a}) \times FAR_{1b}$$

$$+ (1 - FAR_{1a}) \times (1 - FAR_{1b}) \times FAR_{1c}$$

$$FRR_{S1} = FRR_{1a} \times FRR_{1b} \times FRR_{1c}$$

$$FAR_{S2} = FAR_{2a} + (1 - FAR_{2a}) \times FAR_{2b}$$

$$+ (1 - FAR_{2a}) \times (1 - FAR_{2b}) \times FAR_{2c}$$

$$FRR_{S2} = FRR_{2a} \times FRR_{2b} \times FRR_{2c}$$

$$FAR_{SS} = FAR_{S1} \times FAR_{S2}$$

$$FAR_{SS} = FRR_{S1} + (1 - FRR_{S1}) \times FRR_{S2}$$

Turning back to the example with $FAR_{1a,1b,1c} = FRR_{1a,1b,1c} = 5\%$

$$FAR_{2a, 2b, 2c} = FRR_{2a,2b, 2c} = 2\%$$

the following results are obtained.

$$FAR_{SS} = 0.083 \text{ or } 8.3\%$$

$$FRR_{SS} = 0.0013 \text{ or } 0.13\%$$

This set-up thus provide an overall improvement since both the FAR and FRR have better values than the individual systems.

[0028] The theory set out here before shows thus by using several layers into an authentication scheme in a same session enables the combination of several biometric results. Figure 5 shows schematically an embodiment according to the state of the art of combining several bio-engines. The illustrated device comprises face authentication member 1, a fingerprint authentication member 2 and a voice authentication member 3 which are all connected to a Local Area Network 4 (LAN). Of course other members could be connected to the LAN but only three are shown for the sake of clarity. A firewall 5 protects the LAN from the outside publically accessible network 7 to which a netserver 6 is connected. The entity 8 to which access has to be managed is for example formed by an entrance door. Each of the members 1, 2 and 3 operate individually from each other and have there own server and their own database in which biometric templates are stored. Biometric templates being each time formed by a set of data comprising the biometric data belonging to one or more clients of which the access to the entity has to be controlled and who have access to the entity. So for example the biometric template of the face of Arthur Jones who has access to the building is formed by a set of data identifying the face of Arthur Jones.

[0029] In the device of figure 5 each of the members will perform there own authentication process by using their own database and own bio-engines and each bio-engine will issue a score which will be compared with

the threshold set in that bio-engine upon initializing that bio-engine. If the score of the bio-engine is higher than the threshold an acceptance signal will be issued and supplied to the LAN, if not a refusal signal is issued and supplied to the LAN. The score such as issued by the bio-engine is not available on the LAN.

[0030] As already mentioned each bio-engine provides a score which is thresholded to come to a decision being accept, reject or fuzzy. Each bio-engine has a performance curve that characterizes the technology involved and which is expressed by the EER.

[0031] Figure 6 shows a first curve (a) for the bonafide score and a second curve (b) for the impostor score. The vertical line (c) illustrates the set threshold value.

If the score is higher than the threshold the user is accepted, if not he is rejected. In biometrics there is a typical trade-off between accepting users and rejecting them. Increasing the threshold will lower the false accept but will raise the false reject rate. Since biometrics, by their nature, are not deterministic the score obtained by the bio-engines may show variance over time. Typically a user either a bonafide or an impostor, will usually have a Gaussian distribution around his mean score.

[0032] Combining different biometrics, each with their specific FAR, FRR and EER enables to get a better performance. The biometric authentication device according to the present invention combines the outcome of different bio-engines at their result or score level and not at the level of the signals as it is the case for the device shown in figure 5. An example of a biometric authentication device according to the present invention is schematically illustrated in figure 7. The device comprises a LAN 10 to which a layered biometric platform 11 is connected. A firewall 16 is connected between the LAN 10 and the outside network 17 to which a web server 19 could also be connected. Different client modules 12 (a, b, c) can be connected to the platform 11. So for example module 12a is dedicated to particular client features for the LAN security, whereas module 12b respectively 12c is dedicated to particular client features for the web security and physical access to an entity such as a door 13. The different bio-engines performing the biometric authentication operation are now embedded in the platform. The centralization of all bio-engines 11a, 11b and 11c into one platform enables to centralize the storage of the bio-data and templates and to have a common logging and archiving environment. The platform has a common server operating with a common database which is either permanently embedded in the platform and for example formed by a hard disc or another memory, or is formed by a stand alone memory such as for example a smartcard which is connectable to the platform. The server is formed either by a relatively powerful computer, as biometric needs an intensive cpu work, or is formed by different processors provided to operate together.

[0033] Figure 8 illustrates an embodiment of the architecture of the platform and the client module of the

biometric authentication device according to the present invention. The client module 12 comprises one or more data capture units 20, depending on the biometric authentication to be performed. So for example if authentication is to be performed on the face, the fingerprint and the voice, the data capture unit will comprise a camera, a fingerprint scanner and a microphone. The data capture unit is connected with an interface 21 provided to process the data captured by the unit 20 into a predetermined format arranged to be processed by the bio-engines. A client feature unit 22 is further connected to the interface 22 and is provided for input of client dedicated features. Such features indicate for example particularities for certain users (poor quality of the voice, etc.) Which can then be taken into account by the device. The data provided by the client feature unit 22 is also formatted by the interface 21.

[0034] The interface 21 is connected to a bio-application program interface 23 which is part of the platform 11. This platform comprises a decision unit formed by a core server 24 and a module manager 25. The decision unit is connected to interface 23. Different bio-engines 26, 27 and 28 are connected to the decision unit and are operating according to a master-slave relationship, the decision unit being the master and the bio-engines the slaves. The module manager 25 is provided for managing the data traffic between the core server and the bio-engines. Bio-engine 26 executes a voice authentication operation and bio-engines 27 and 28 respectively execute a face and a fingerprint authentication. Of course more than three bio-engines could be available and even with two bio-engines the invention could be applicable. It should also be noted that the decision unit can operate on different operating systems, being Windows, Unix etc.

[0035] The decision unit is also connected with a first bio-decision engine 29 provided for executing a serial combinatorial operation with the scores of at least one bio-engine. Bio-decision engine 29 for example can apply an AND operation on the scores of bio-engine 26 or on the scores of bio-engines 26 and 27. The decision unit is further connected with a second bio-decision engine 30 provided for executing a parallel combinatorial operation, i.e. applying an OR operation, with the scores of at least one bio-engine. The first and second bio-decision engines are also slaves for the decision unit. It should be noted that the presence of both the first and the second bio-decision engines is not absolutely required. The device according to the present invention could also operate with only one of those bio-decision engines or even with none of the bio-decision engines.

[0036] A data base manager 31 is also connected to the decision unit. This data base manager controls the data traffic between the decision unit and a database 32 wherein the biometric templates of the clients are stored. A self learning module 33 is further connected to the decision unit and is provided for updating the templates stored in the data base as a result of one or more

good scores issued by the bio-engine. Finally an environmental module 34 to which sensors 35 and 36 are connected, is connected to the decision unit. The latter module is provided for supplying environmental information to the decision unit such as for example background noise which could adversely affect the signal picked up by the microphone, or heavy light intensity which could adversely affect the image recorded by the camera. The sensors 35 and 36 are then formed by a dB meter and a light intensity meter and supply their measurement values to the environmental module 34. The latter then interprets these values and forwards information to the decision unit which thereupon can modify its decision criteria as will be described hereinafter.

[0037] Before the biometric authentication device according to the present invention is fully operative an initialisation process is required. The initialisation process comprises the loading of the client features by means of the client features unit 22. Once loaded they are formatted by the interface 22 and forwarded to the decision unit (24, 25). The biometric templates of the users also have to be created and stored into the database. For this purpose each of the users to who access will be provided to the entity protected by the device, will have to present themselves to the data capture unit so that the necessary data can be collected to form the templates. Once the data capture unit has collected the data from the user, this data is formatted into a biometric template according to a predetermined format by the interface 21 and forwarded via the decision unit and the database manager 31 to the database where the template is stored. If the database stores the templates of several users, a PIN (Personal Identification Number) is assigned to each user and the value of the PIN is stored in the database together with the templates to which the PIN belongs. If a smartcard is used as database the use or manual entry of a PIN is not necessarily required as the user carries this smartcard with him and only needs to insert his smartcard into the device to furnish his template and his supposed identity stored on the smartcard to the device. In order to enable a suitable operation of the device, it is of course necessary that the templates are formatted in a same way as will be the data collected by the data capture unit for an authentication operation.

[0038] The initialisation further comprises the initialisation of the decision unit which is loaded with weight factors to be assigned to the scores issued by the bio-engines as well as the relationship between those weight factors. The threshold value of the device also has to be set, as this will be dependent of the level of security desired.

[0039] The operation of the biometric authentication device according to the invention will now be described with reference to a flowchart shown in figure 9. Suppose a bonafide user wants to get access to an entity protected by the biometric authentication device. The user presents (40) himself in front of the device and types (49) his PIN and/or introduces (41) his smartcard com-

prising his templates. The client module 12 will open (42, 45) an authentication session by activating the data capture unit 20 and reading the introduced PIN and/or the templates available on the smartcard. When a PIN is received the template associated to that PIN is read (46) in the database and supplied to the database manager 32. If the PIN is incorrect, which could be the case with an impostor or due to an error during typing, an error message is generated which can start a retry operation. After a predetermined number of retries, for example threes the device sends a refusal message and access is refused.

[0040] The data capture unit will capture (43) life biometric data from the user, for example by letting him say a predetermined word, for example his name, recording a picture from his face and fingerprint. The captured data is formatted (44) by the interface 21 in order to form a life biometric database which is the supplied (45) to the decision unit.

[0041] The core server of the decision unit is provided to form a decision based on a decision strategy. This strategy comprises the processing of the scores such as issued by the bio-engines 26, 27 and 28. Suppose for example that the Verified Score to be generated by the decision unit is formed by : $V_s = \alpha S_v + \beta S_f + \gamma S_p$ wherein

S_v : score generated by the bio-engine 26 performing the voice authentication

S_f : score generated by the bio-engine 27 performing the face authentication

S_p : score generated by the bio-engine 28 performing the fingerprint authentication

and α , β and γ being weight factors comprised between 0 and 1 and $\alpha + \beta + \gamma = 1$

The scores of the bio-engines being normalized - $1 \leq S \leq +1$

The decision unit will then issue either an acceptance if $V_s > Th$ or a refusal if $V_s \leq Th$, where Th is the threshold value. The values given here are only given by way of example and it will be clear that other values can be used as well as other mathematical relationships for V_s and for the weight factors.

[0042] The life biometric data supplied to the decision unit is forwarded (47) by using the module manager 25 to the respective bio-engines. The module manager also forwards the biometric templates retrieved from the data base to the respective bio-engines. So the voice template and voice life biometric data is forwarded to the bio-engines 26 and respectively the face and the fingerprint data to the bio-engines 27 and 28 respectively. The bio-engines then perform (50) their authentication operation on the received data and generate each a respective score S_v , S_f , S_p .

[0043] Depending on the configuration of the device, the module manager sends the scores to the core server if only one authentication procedure is necessary, or to

the bio-decision engines 29 or 30 if serial or parallel combinatorial operations are requested (48). In the latter case the bio-engines will again perform one or more authentication operations in function of how much attempts are involved in the serial an/or parallel combinatorial operation. In case of combinatorial operations the module manager preferably supplies new life biometric data captured by the data capture unit. The bio-decision engines then perform (51) their combinatorial operation on the scores of the bio-engines and determine a value for S_v , S_f and S_p which is supplied via the module manager to the core server.

[0044] Once the core server has received the score values, the verified scores V_s is determined and compared with the threshold value Th . If $V_s > Th$ the core server issues (52) an acceptance signal and enables (54) access. If $V_s \leq Th$ the core server either issues a refusal or starts a retry (53) depending on how the latter is configured.

[0045] If the core server is configured for starting a retry operation it will generate a control signal in order to start such a retry operation. Under control of such a control signal the weight factors α , β or γ can then be adjusted and further weight factors α' , β' and γ' are generated. This adjustment is for example done by taking into account the score values and/or the client feature. If for example the client feature indicates that the concerned user has a poor voice quality, the weight factor α is reduced for example by 25 % and the others are increased in order to satisfy the criteria $\alpha + \beta + \gamma = 1$. On the other if the score of the face is for example excellent, i.e. substantially higher than the threshold Th_f for the face, and the one of the voice is normal whereas the one of the fingerprint is bad, for example because the finger is injured or burned, the core server can decide to lower γ and increase β . The core server then determines again V_s by using the further weight factors and not necessarily by starting a new authentication process. If $V_s > Th$ an acceptance signal is generated. if not again a retry (53) can be generated or the process is stopped.

[0046] The original aspect of the present device is thus to move the decision to verify and/or identify a user out of the several single bio-engines and to let them operate as slaves of a decision unit where the final decision is taken based on weighted individual scores. The bio-engine as such can no longer alone decide to accept or reject, because their score value is no longer individually checked against a threshold value. Only the verified score, such as obtained and processed by the decision unit, can decide on accept or reject.

[0047] If the device comprise a self learning module 33, the latter is informed by the core server 24 if a bio-engine issues a very high score. This signifies that probably the life biometric data is of exceptional quality. To that purpose the core server for example generates a second control signal when the score of the considered bio-engine is higher than a further threshold value which

is for example 20 % higher than the threshold of that bio-engine. The self learning module will then ask the module manager to furnish this life biometric data and will substitute the template stored in the database by this life biometric data which will now form the biometric template.

[0048] If the device comprises an environmental module 34, the information generated by that module is furnished to the core server under control of a trigger signal generated by that module. The core server is then provided to modify the weight factors α , β and γ in function of the received information and under control of the trigger signal. For example if a heavy background noise is detected, the dB meter will indicate a high value and the core server can decrease the value of α depending on the measured dB value.

Claims

1. A biometric authentication device provided for managing access to at least one entity, said device being operatively connectable to a database provided for storing biometric templates, said device comprising a set of bio-engines each having an input for receiving said biometric templates and life biometric data originating from a data capture unit provided to collect life biometric data, each of said bio-engines being provided for performing a dedicated biometric authentication operation with said biometric templates and said life biometric data and for generating a score as a result of said authentication operation, characterized in that said device comprises a decision unit connected to said bio-engines and operating according to a master-slave relationship, wherein said decision unit being the master, said decision unit being provided for receiving each of said scores and for assigning a respective weight factor to each of said scores and forming a set of weighted scores therewith, said decision unit being further provided for combining said weighted scores and generating a verified score therewith, said decision unit being also provided for comparing said verified score with a threshold value and for generating an access enable signal as a result of a positive comparison and an access refusal signal as a result of a negative comparison.
2. A biometric authentication device as claimed in claim 1, characterized in that the decision unit is connected with a first bio-decision engine, which is provided for executing a serial combinatorial operation with the scores generated by at least one of said bio-engines, said first bio-decision engine being provided to operate as a slave from said decision unit.
3. A biometric authentication device as claimed in claim 1 or 2, characterized in that the decision unit is connected with a second bio-decision engine, which is provided for executing a parallel combinatorial operation with the scores generated by at least one of said bio-engines, said second bio-decision engine being provided to operate as a slave from said decision unit.
4. A biometric authentication device as claimed in anyone of the claims 1 to 3, characterized in that said decision unit is provided for generating a control signal when said verified score is below said threshold, said decision unit being further provided for determining a set of further weight factors under control of said control signal and assigning them to said scores and generating a further verified score therewith.
5. A biometric authentication device as claimed in claim 4, characterized in that said further weight factors and said weight factors each time satisfy a predetermined relationship.
6. A biometric authentication device as claimed in anyone of the claims 1 to 5, characterized in that said decision unit comprises a core server which is provided for generating said verified score and executing said comparison.
7. A biometric authentication device as claimed in claim 6, characterized in that said decision unit comprises a module manager which is provided for managing data traffic between said bio-engines and said core server.
8. A biometric authentication device as claimed in claim 2 and 6 or 3 and 6, characterized in that said decision unit comprises a module manager, which is provided for managing data traffic between said bio-decision engine and said core server.
9. A biometric authentication device as claimed in anyone of the claims 1 to 8, characterized in that said data capture unit is connected to an interface to which a feature module is connected, said feature module being provided for input of client dedicated features.
10. A biometric authentication device as claimed in anyone of the claims 1 to 9, characterized in that said biometric templates are stored on a memory formed by either a smartcard, a harddisk, a EEPROM or a flash memory.
11. A biometric authentication device as claimed in anyone of the claims 1 to 10, characterized in that said device comprises an interface having an input for receiving said life biometric data from said data capture unit.

ture unit, said interface being provided to format said life biometric data according to a predetermined format.

12. A biometric authentication device as claimed in anyone of the claims 1 to 11, characterized is that said decision unit is connected to a self learning module which is provided for substituting into said database a biometric template by a life biometric data under control of a second control signal generated by said decision unit upon detection of a score issued by a bio-engine which is higher than a further predetermined threshold value.

13. A biometric authentication device as claimed in anyone of the claims 1 to 12, characterized in that said decision unit is connected to an environmental module which is provided for generating a trigger signal, said decision unit being provided to modify the weight factors under control of said trigger signal.

5
10
15
20
25
30
35
40
45
50
55

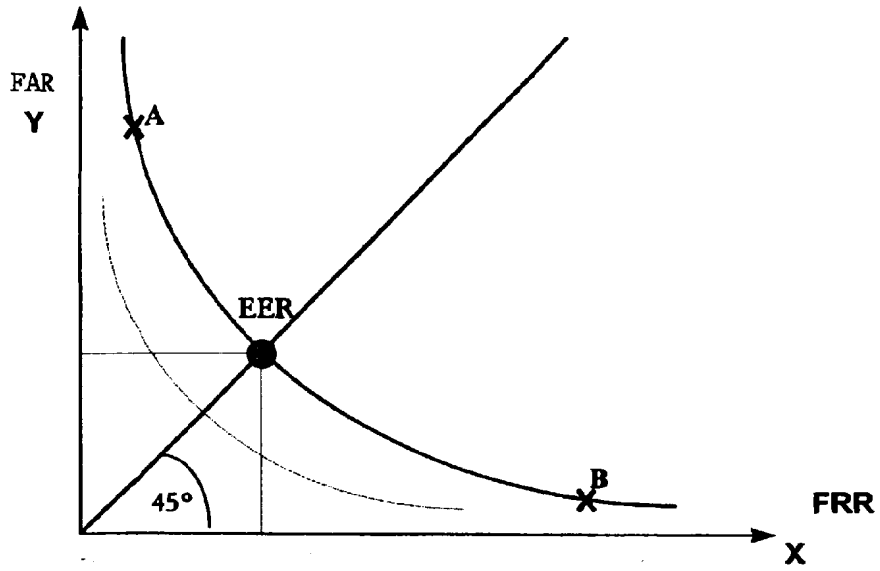


Fig. 1

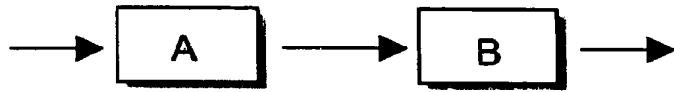


Fig. 2

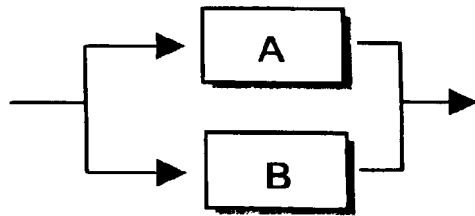


Fig. 3

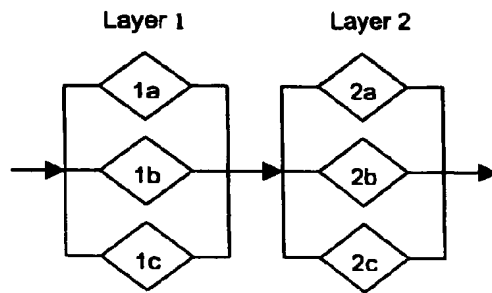


Fig. 4

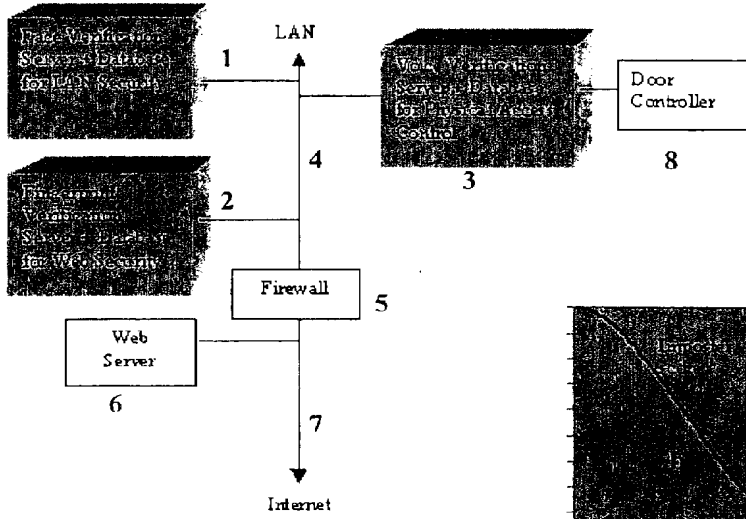


Fig. 5

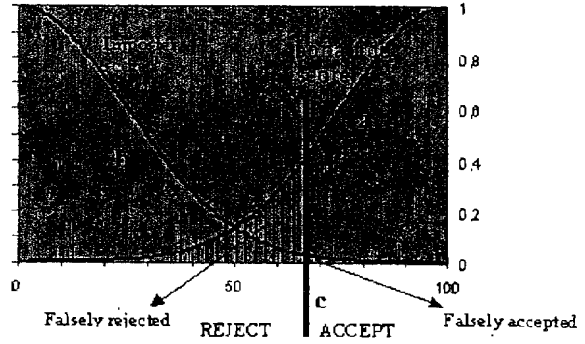


Fig. 6

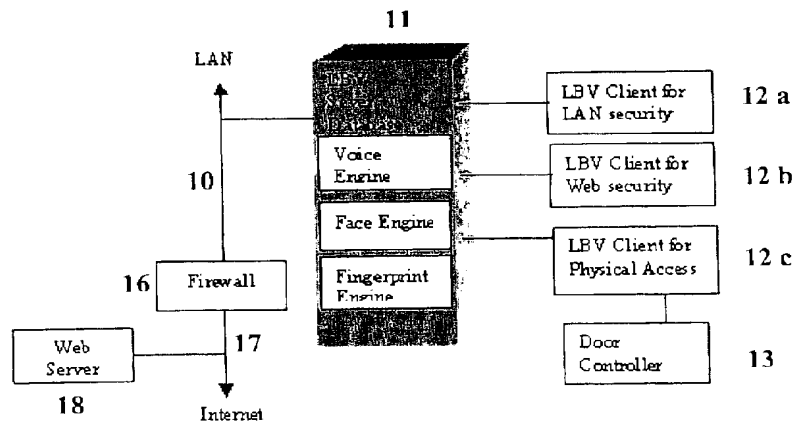


Fig. 7

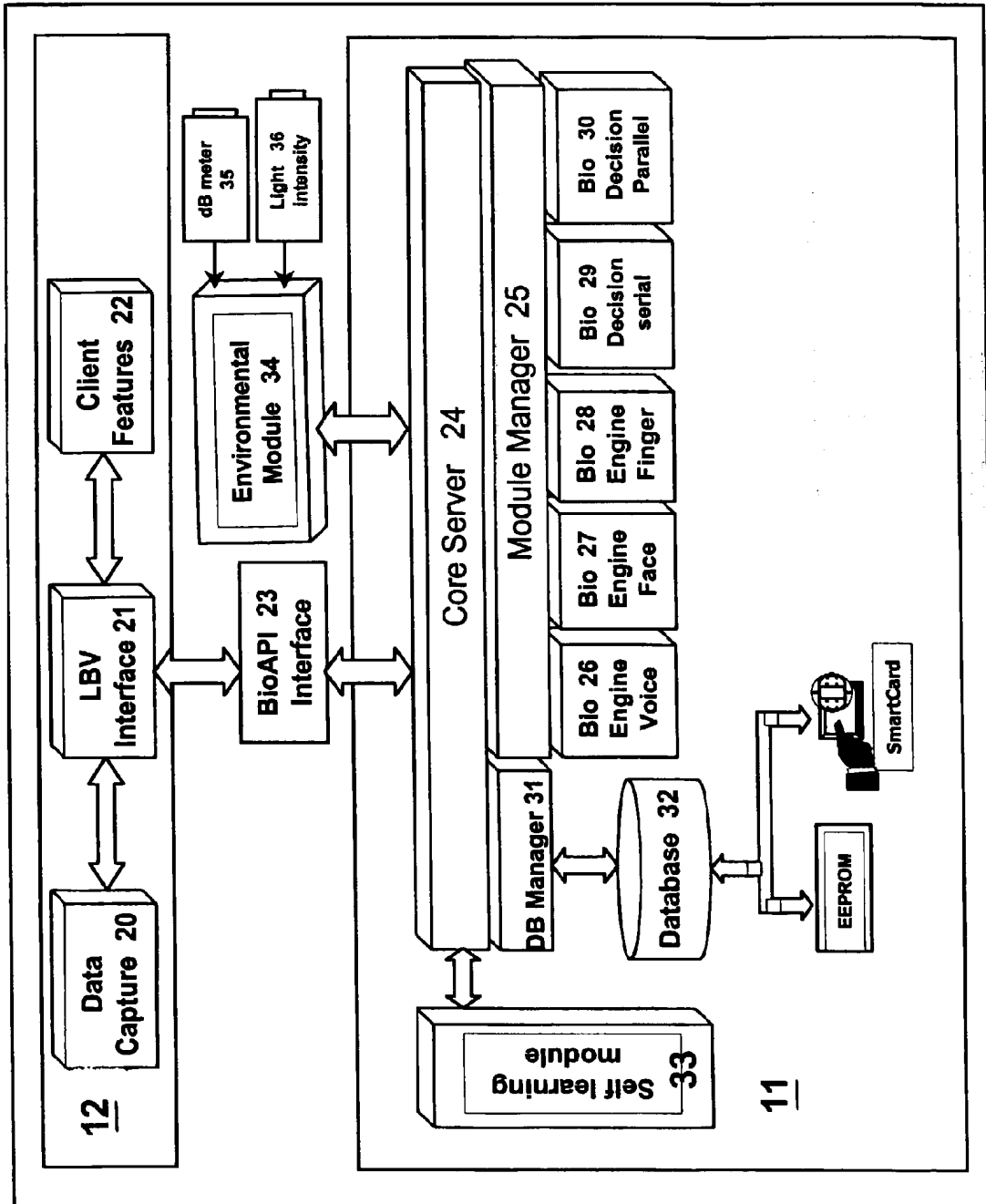
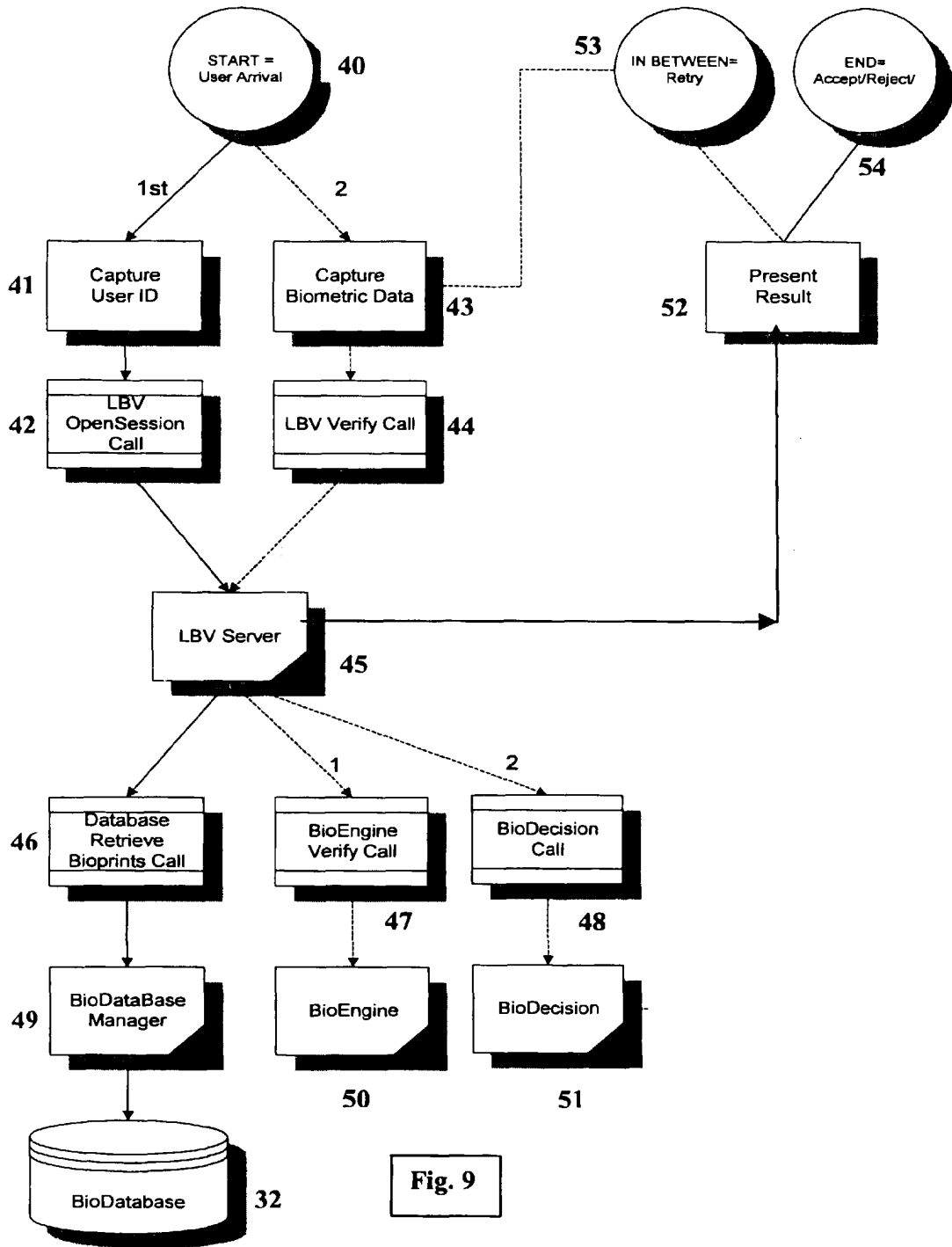


Fig. 8





European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 99 87 0178

DOCUMENTS CONSIDERED TO BE RELEVANT			
Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
A	WO 95 26013 A (MINNESOTA MINING & MFG) 28 September 1995 (1995-09-28) * claim 1; figure 1 *	1-13	G06K9/68
A	LUO R C ET AL: "A TUTORIAL ON MULTISENSOR INTEGRATION AND FUSION" PROCEEDINGS OF THE ANNUAL CONFERENCE OF THE INDUSTRIAL ELECTRONICS SOCIETY. (IECON),US,NEW YORK, IEEE, vol. CONF. 16, 1990, pages 707-722, XP000217315 ISBN: 0-87942-600-4 * the whole document *	1-13	
A	GB 2 229 305 A (BRITISH TELECOMM) 19 September 1990 (1990-09-19) * abstract; figure 1 *	1-13	
A	FR 2 634 570 A (ANDRE CATHERINE ;REITTER RENAUD (FR); REVILLET MARIE JOSEPHE (FR)) 26 January 1990 (1990-01-26) * the whole document *	1-13	
			TECHNICAL FIELDS SEARCHED (Int.Cl.7)
			G06K
The present search report has been drawn up for all claims			
Place of search		Date of completion of the search	Examiner
THE HAGUE		4 February 2000	Granger, B
CATEGORY OF CITED DOCUMENTS			
X : particularly relevant if taken alone Y : particularly relevant if combined with another document of the same category A : technological background O : non-written disclosure P : intermediate document		T : theory or principle underlying the invention E : earlier patent document, but published on, or after the filing date D : document cited in the application L : document cited for other reasons & : member of the same patent family, corresponding document	

EPO FORM 1503 03.82 (P/MC01)

ANNEX TO THE EUROPEAN SEARCH REPORT
ON EUROPEAN PATENT APPLICATION NO.

EP 99 87 0178

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

04-02-2000

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9526013 A	28-09-1995	AU 2186095 A	09-10-1995
		BR 9507142 A	30-09-1997
		CA 2183886 A	28-09-1995
		DE 69501327 D	05-02-1998
		DE 69501327 T	23-07-1998
		EP 0752143 A	08-01-1997
		ES 2110841 T	16-02-1998
		JP 9510636 T	28-10-1997
		US 5719950 A	17-02-1998
		-----	-----
GB 2229305 A	19-09-1990	HK 127496 A	26-07-1996
-----	-----	-----	-----
FR 2634570 A	26-01-1990	NONE	
-----	-----	-----	-----

EPO FORM P0469

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

(19)



Europäisches Patentamt

European Patent Office

Office européen des brevets



(11)

EP 0 986 209 A2

(12)

EUROPEAN PATENT APPLICATION

(43) Date of publication:
15.03.2000 Bulletin 2000/11

(51) Int. Cl.⁷: **H04L 9/32**

(21) Application number: 99112066.8

(22) Date of filing: 22.06.1999

(84) Designated Contracting States:
**AT BE CH CY DE DK ES FI FR GB GR IE IT LI LU
MC NL PT SE**
Designated Extension States:
AL LT LV MK RO SI

(30) Priority: 11.09.1998 JP 25781398

(71) Applicant:
**mitsubishi denki kabushiki kaisha
Tokyo 100-8310 (JP)**

(72) Inventors:
• **Nakamura, Hiroshi,
c/o Mitsubishi Denki K.K.
Tokyo 100-8310 (JP)**

- **Fujii, Teruko,
c/o Mitsubishi Denki K.K.
Tokyo 100-8310 (JP)**
- **Sadakane, Tetsuo,
c/o Mitsubishi Denki K.K.
Tokyo 100-8310 (JP)**
- **Baba, Yoshimasa,
c/o Mitsubishi Denki K.K.
Tokyo 100-8310 (JP)**

(74) Representative:
**Pfenning, Meinig & Partner
Mozartstrasse 17
80336 München (DE)**

(54) Remote authentication system

(57) To obtain a remote authentication system that securely authenticates with protecting biometrics information, which is user's personal information, and is firm on security when performing authentication of a person with the biometrics information, and a remote authentication method. The present invention encrypts biometrics information that is user's personal information, and transfers the biometrics information over a network in such a state that only an authentication server, which the user assigns, can decode the biometrics information. Therefore, it is possible to securely protect user's privacy that is the biometrics information in a style of reflecting user's intention, and to prevent reuse of invalid authentication information since it is possible to confirm the date and time, when the authentication information was generated, by the authentication server. Furthermore, it is possible to keep the security of a system firm since an authenticated side can confirm whether the user is authenticated.

EP 0 986 209 A2

Description

BACKGROUND OF THE INVENTION

1. Field of the Invention

[0001] The present invention relates to a remote authentication system identifying a person with biometrics.

2. Description of the Related Art

[0002] Heretofore, so as to perform security protection in an information processing system connected to a network, it is necessary to identify a person and to judge approval or disapproval of access of the person, that is, to perform authentication. In addition, in cash dispensers of banks and the like, authentication for identifying a person and accessing the person's transaction information, and authentication for entrance into and exit from confidential research sites, membership clubs, and the like, which have high confidentiality, are performed.

[0003] Identification of a person and authorization of the person's qualification, that is, authentication is performed with a magnetic card, an IC card, which are positioned similarly to an identification card and the like, and the person's memory such as a password, and combination of them. There are problems that the authentication cannot be performed because the password is forgotten, and the magnetic card and IC card are lost or broken, and another person, who is not the principal, is authenticated with masquerading by burglary and leakage of password information.

[0004] In addition, as one of means for authenticating a user over a network, there is a digital signature for indirectly authenticating the user by authenticating a message created by the user. In the digital signature, first, a message sender attaches a cryptogram that is encrypted from a message digest, into which an original message is compressed, with the sender's cryptographic key to the message. A message receiver confirms that the message is one, which the sender himself/herself sent, and that the message is not tampered, by creating a message digest from the message received, decoding the message digest from the cryptogram, which is attached, with the sender's decoding key, and confirming coincidence of these two message digests.

[0005] In addition, in the above-described encryption method, there are a common key encryption method, using the same key for a cryptographic key and a decoding key, and a public key encryption method using different keys for the cryptographic key and decoding key. In the public key encryption method, when one key is set as a secret key and is kept safely and another key is officially announced as a public key, the cryptogram encrypted with the public key cannot be decoded into the original message if a receiver has not the secret key,

and hence the sender can transfer the message in such a form that only the receiver, who is desired by the sender, can decode, and the cryptogram encrypted with the secret key can be decoded with the public key into the original message, and hence the receiver can authenticate that the message is one from the sender herself/himself having the secret key.

[0006] Heretofore, although, in RFC1421 and RFC1422 (PEM: Privacy Enhancement for Internet Electronic Mail) that are registered in RFC (Request For Comment) of IETF (Internet Engineering Task Force), the digital signature and message encryption are performed with the public key encryption method and common key encryption method, there is a problem that it is necessary to administrate the secret key on the sender's hands since the sender uses the own secret key, for example, to safely keep the secret key with saving the secret key in a floppy disk, a magnetic card, and an IC card.

[0007] On the other hand, in the authentication with biometrics information, which is a person's biological characteristic such as finger print information, palm print information, handwriting information, and retina information, it is difficult to perform masquerade and is unnecessary to administrate the information of the secret key so long as the user himself/herself presents, and it is possible to resolve the complexness of keeping a baggage and the threat of loss at the time of the authentication of a person and the complexness of memory at the time of the authentication of a password with the magnetic card and IC card. Nevertheless, there are problems that, if the authentication with the biometrics information is necessary in a wide range, the equipment for performing the centralized administration and authentication of the biometrics information is necessary, and that it is necessary to keep security with concealing the user's biometrics information at the time of transferring the biometrics information to the equipment, performing the authentication, from the viewpoint of protection of privacy.

[0008] Furthermore, in general, random numbers are for creating a cryptographic key in a system creating the cryptographic key used for concealing the biometrics information. Nevertheless, there is also a problem that it is important to eliminate the tendency of the random numbers so as to make it difficult to break the cryptographic key.

[0009] In addition, an apparatus acquiring biometrics should be properly administrated from the viewpoint of protection of users' privacy, and it is necessary to authenticate an administrator. Nevertheless, there is a problem that, since another person cannot act for the administrator if the authentication of this administrator was performed with biometrics, another person can never perform the access to the biometrics acquisition apparatus including initialization. Furthermore, there is a problem that even a valid administrator can never perform the access to the biometrics acquisition apparatus

including initialization if the biometrics used for the authentication is largely changed or lost by suffering damage in an accident in case of the valid administrator.

[0010] Moreover, in general, a system performing user authentication is required to early find an invalid authentication, for example, as for a cash card in a bank, there is means for making a cash card unusable if authentication with a preset number of times of password inputs is unsuccessful. Also, a user authentication system with the biometrics is required to early find an invalid authentication. Nevertheless, a condition of biometrics is different every person, for example, in a system authenticating a person with finger print matching, a minimum matching rate identifying a person as the principal is determined, but a person whose finger is rough or worn gets a low matching rate even if the person can obtain the best biometrics information at that time, and a failure probability of the authentication itself increase if the matching rate decreases due to a minor failure such as insufficient contact at the time of acquiring the finger print. Therefore, there is a problem that it cannot be equally performed for all the persons that it is judged to be an unsuccessful authentication within only the preset number of times.

SUMMARY OF THE INVENTION

[0011] The present invention is to solve above problems, and an object of the present invention is to provide a remote authentication system which securely authenticates with protecting biometrics information, which is user's personal information, and is firm on security when performing authentication of a person with the biometrics information, and a remote authentication method.

[0012] In a remote authentication system, in which an authentication server, an application server, and a user terminal are connected to a network respectively, and which authenticates a user using the user terminal, a remote authentication system according to a first invention is a system, wherein the authentication server has a pair of a public key and a secret key in a public key encryption method, announces the public key, and conceals the secret key; wherein at least one kind or a plural kind of biometrics acquisition apparatus is connected to the user terminal; wherein the biometrics acquisition apparatus: encrypts user's biometrics information, acquired at the time of authentication, with a common key in a common key encryption method; acquires date and time information, creates a message digest with connecting the date and time information with the common key, and further encrypts the message digest with the common key; acquires the public key of the authentication server, which the user assigns, and encrypts the common key with the public key of the authentication server; and transfers the biometrics information encrypted, the common key and date and time information, which is encrypted, and the message digest

encrypted with connecting the date and time information with the common key, as authentication information to the user terminal; and wherein the user terminal and application server transfer the authentication information to the authentication server, and the authentication server: decodes user's biometrics information with the common key acquired by decoding the authentication information, which is transferred, with the secret key; authenticates the user with the biometrics information; and encrypts result of authentication and a message digest of the result of the authentication with the secret key and transfers both to the application server.

[0013] In addition, in a remote authentication system, in which an authentication server and a user terminal are connected to a network respectively, and which authenticates a user using the user terminal, a remote authentication system according to a second invention is a system, wherein the authentication server has a pair of a public key and a secret key in a public key encryption method, announces the public key, and conceals the secret key; wherein at least one kind or a plural kind of biometrics acquisition apparatus is connected to the user terminal; wherein the biometrics acquisition apparatus: encrypts user's biometrics information, acquired at the time of authentication, with a common key in a common key encryption method; acquires date and time information, creates a message digest with connecting the date and time information with the common key, further encrypts the message digest with the common key; acquires the public key of the authentication server, which the user assigns, and encrypts the common key with the public key of the authentication server; and transfers the biometrics information encrypted, the common key and date and time information, which is encrypted, and the message digest encrypted with connecting the date and time information with the common key, as authentication information to the user terminal; wherein the user terminal transfers the authentication information to the authentication server; and wherein the authentication server: decodes user's biometrics information with the common key acquired by decoding the authentication information, which is transferred, with the secret key; authenticates the user with the biometrics information; and encrypts result of authentication and a message digest of the result of the authentication and transfers both to the user terminal.

[0014] In addition, a remote authentication system is a system, wherein a biometrics acquisition apparatus: transfers biometrics information to a user terminal without encrypting the biometrics information at the time of authentication; encrypts the user's biometrics information, which the user terminal obtains, with a common key in a common key encryption method; acquires date and time information, creates a message digest with connecting the date and time information with the common key, encrypts the message digest with the common key; acquires a public key of an authentication server,

which the user assigns; encrypts the common key with the public key of the authentication server; and transfers the biometrics information encrypted, the common key and date and time information, which is encrypted, and the message digest encrypted with connecting the date and time information with the common key, as authentication information.

[0015] Furthermore, a remote authentication system according to a fourth invention uses biometrics information as a part or all of random numbers for creating a common key in a common key encryption method for encrypting the user's biometrics information acquired, at the time of authentication.

[0016] A remote authentication system according to a fifth invention is a system, wherein a biometrics acquisition apparatus includes; an authentication unit of an administrator administrating the biometrics acquisition apparatus; and an authentication unit of an initializer initializing the biometrics acquisition apparatus, wherein the two authentication units perform authentication separately, and can perform only the initialization with authentication of the initializer.

[0017] A remote authentication system according to a sixth invention is a system, wherein an authentication server: saves historic records of matching rates that are results of matching biometrics at the time of user authentication; compares a matching rate with an average matching rate at the time of identifying a user as a principal until the previous occasion if the authentication server does not identify the user as the principal at the time of user authentication; confirms whether the matching rate at this time changes more largely than a preset value determined by an administrator; and informs a contact, who is registered beforehand, if a number of failed times due to changes more largely than the fixed value reaches a fixed value determined by the administrator.

[0018] A remote authentication system according to a seventh invention is a system, wherein an authentication server: saves historic records of matching rates that are results of matching biometrics at the time of user authentication; compares a matching rate with a matching rate at the time of identifying a user as a principal until the previous occasion at the time of user authentication if the authentication server identifies the user as the principal; makes the user authentication unsuccessful if the two matching rates are the same rates and a message digest of biometrics information is not saved, performs message digest calculation of biometrics information at this time, saves the message digest of biometrics information with the matching rate; saves a message digest of biometrics information at this time with a matching rate as a pair with calculating the message digest of biometrics information at this time if the two matching rates are the same and a message digest is saved, compares the message digest of biometrics information at this time with the message digest of biometrics information at the same matching rate in the

past, identifies the user as a principal if both message digests are different from each other; does not identify the user as a principal if a pair of a matching rate and a message digest at this time completely coincides with a pair of a matching rate and a message digest in the past; and informs a contact, who is registered beforehand, if a number of cases that the pair of the matching rate and message digest at this time completely coincides with the pair of the matching rate and message digest in the past reaches a value equal to or larger than a fixed value which is determined by an administrator.

BRIEF DESCRIPTION OF THE DRAWINGS

[0019]

Fig. 1 is a block diagram showing the configuration of a first embodiment of an Web system where a remote authentication system according to the present invention is applied;

Fig. 2 is a timing chart for explaining the processing of authentication in the Web system in Fig. 1;

Fig. 3 is a block diagram showing the configuration of a second embodiment of a database retrieval system where a remote authentication system according to the present invention is applied;

Fig. 4 is a timing chart for explaining the processing of authentication in the database retrieval system in Fig. 3;

Fig. 5 is a block diagram showing the configuration of a third embodiment of an Web system where a remote authentication system according to the present invention is applied;

Fig. 6 is a timing chart for explaining the processing of authentication in the Web system in Fig. 5;

Fig. 7 is a block diagram showing the configuration of a fourth embodiment at the time of administration of a finger print acquisition apparatus where a remote authentication system according to the present invention is applied;

Fig. 8 is a block diagram showing the configuration of a fifth embodiment of an authentication server where a remote authentication system according to the present invention is applied.

DESCRIPTION OF THE PREFERRED EMBIDIMENTS

[0020] Hereinafter, embodiments of the present invention will be described with reference to drawings.

Embodiment 1.

[0021] Fig. 1 shows the configuration of a Web system 1 where the present invention is applied. Over a network 2, an authentication server 3, an Web server 4 that is an application server, and a user terminal 5 are connected, and a biometrics acquisition apparatus 6 is connected to the user terminal 5. In this Web system 1, if a user

accesses the Web server 4 through the user terminal 5, the Web server 4 receives user's personal authentication from the authentication server 3, and according to the result, the Web server 4 performs access control to the user.

[0022] The authentication server 3 is a computer system (hereinafter, this is shown as a system having a CPU, memory, a disk, communication control, and the like) such as a personal computer and a workstation that are composed of an authentication controller 3A, an encryption processing unit 3C, and an authentication information database 3B, and announces one key in a public key method as a public key and conceals another key as a secret key.

[0023] In addition, the Web server 4 is a computer system such as a personal computer and a workstation where a Web server database 4A, an encryption processing unit 4D, an authentication request unit 4B, and an application of a Web server software 4C (hereinafter, software is written as S/W) that is an application requiring personal authentication operate.

[0024] In addition, the user terminal 5 is a computer system such as a personal computer and a workstation where a browser 5A displaying information of the Web server terminal 4, and authentication information acquisition S/W 5B operate. Furthermore, a biometrics acquisition apparatus 6 is connected to the user terminal 5. The biometrics acquisition apparatus 6 represents a finger print acquisition apparatus 7 and a palm print acquisition apparatus 8 that acquire finger print of a human body and palm print information with image processing as biometrics information, a character recognition tablet 9 acquiring handwriting information, which a user draws, as biometrics information, a retina acquisition apparatus 10 acquiring retina information of a human body as the biometrics information with eyeground (fundus) scanning and the like, and the like.

[0025] Here, a case that the finger print acquisition apparatus 7 is used as the biometrics acquisition apparatus 6 will be described as an example. In addition, the biometrics information acquired by the biometrics acquisition apparatus 6 such as the finger print acquisition apparatus 7 can be image data, image data that is not processed such as electrostatic data, and characteristic point data obtained by extracting characteristics from image data. The finger print acquisition apparatus 7 is composed of a finger print information acquisition unit 7A acquiring finger print information with image processing and the like and transferring the finger print information to the user terminal, an encryption processing unit 7B encrypting the finger print information, and a public key acquisition unit 7C acquiring a public key of the authentication server 3.

[0026] Next, operation will be described.

[0027] A flow of authentication processing in the Web system 1 like this is shown in Fig. 2.

[0028] First, a case (SP5) that a user accesses information in the Web server database 4A, which has high

confidentiality, in the Web server 4 with the browser 5A that is an application operating in the user terminal 5 will be described. The Web server S/W 4C, which is an application performing access control of the information having high confidentiality, is required to perform the user authentication so as to judge whether the user has an access authority.

[0029] The authentication information acquisition S/W 4C in the user terminal 5 acquires the finger print information, which is biometrics information necessary for the authentication, from the finger print acquisition apparatus 7 (SP6). At this time, the S/W 4C may operate with cooperating with other S/W (software such as a driver acquiring the authentication information).

[0030] The finger print information acquisition unit 7A in the finger print acquisition apparatus 7, which is instructed to acquire the finger print information by the authentication information acquisition S/W 5B in the user terminal 5, acquires the finger print information from the user (SP1). Although the encryption processing unit 7B encrypts this finger print information since this finger print information is user's inherent personal information, first, the encryption processing unit 7B creates a common key in the common key method for encrypting this finger print information, and encrypts the finger print information with this common key. At the same time, the encryption processing unit 7B acquires date and time information, creates a message digest with connecting the date and time information with the common key, and further encrypts the message digest with the common key (SP2).

[0031] The public key acquisition unit 7C in the finger print acquisition apparatus 7 acquires a public key of the authentication server from user's instruction such as a floppy disk, a magnetic card, an IC card, or key entry. Alternatively, if the finger print acquisition apparatus 7 is properly administrated, the public key of the authentication server 3 is fixedly saved in the public key acquisition unit 7C in the finger print acquisition apparatus 7, and hence the user may use the public key after recognizing the public key. Next, the encryption processing unit 7B encrypts the common key with the public key of the authentication server 3 (SP3).

[0032] Then, the finger print acquisition unit 7A transfers the finger print information encrypted, the date and time information, the message digest with connecting the date and time information with the common key that is encrypted, and the encrypted common key as the authentication information to the authentication information acquisition S/W 5B in the user terminal 5 (SP4).

[0033] The authentication information acquisition S/W 5B in the user terminal 5 transfers the authentication information, which is acquired, to the Web server 4 through the browser 5A. At this time, the browser 5A transfers the authentication information with adding a user ID such as a user name and a mail address, which the browser 5A acquires separately (SP7).

[0034] The authentication request unit 4B in the Web

server 4 transfers the authentication information, which the authentication request unit 4B acquires through the Web server S/W 4C, to the authentication controller 3A in the authentication server 3 (SP9).

[0035] The authentication controller 3A in the authentication server 3 makes the encryption processing unit 3C decode the authentication information transferred, and performs the user authentication. At this time, the encryption processing unit 3C compares the message digest created from the date and time information and common key, which are transferred, in the authentication server 3 with the message digest decoded from the message digest created with connecting the date and time information, which is encrypted, with the common key, and confirms the validity of the date and time, when the authentication information was created, in consideration of transfer delay (SP12).

[0036] The authentication controller 3A performs finger print matching from the finger print information and user ID, which are included in the authentication information transferred, and personal information originally saved in the authentication information database 3B in the authentication server 3. The authentication controller 3A creates the result of the authentication showing that the user is valid if the authentication controller 3A identifies the user as the principal in consequence of matching, or judges that the user is not the principal if the authentication controller 3A cannot identify the user as the principal in consequence of the matching, and creates the result of the authentication. This result of the authentication is delivered to the encryption processing unit 3C, and the encryption processing unit 3C creates a message digest of the result of the authentication, encrypts the message digest with the secret key of the authentication server 3, that is, performs digital signature, and delivers this message digest, which is encrypted, to the authentication controller 3A. The authentication controller 3A informs the authentication request unit 4B in the Web server 4 of the result of the authentication with including the message digest, which is encrypted, in the result of the authentication (SP13).

[0037] The authentication request unit 4B in the Web server 4 that receiving the result of the authentication informs the encryption processing unit 4D of the result of the authentication. The encryption processing unit 4D decodes the informed message digest, which is encrypted, with the public key of the authentication server 3, and confirms that the message digest is surely the valid message from the authentication server 3 by comparing the decoded message digest with the message digest of the informed result of the authentication (SP10). If the authentication request unit 4B is informed from the encryption processing unit 4D that the encryption processing unit 4D confirmed that the information was the valid information from the authentication server 3, the authentication request unit 4B informs the Web server S/W 4C of the result of the authentication. The Web server S/W 4C judges approval or disapproval of

access to the information in the Web server database, which has high confidentiality, to the user according to the result of the authentication (SP11). For example, the Web server S/W 4C performs operation to the user access such as the display of the confidential information.

[0038] In this manner, the finger print information that is user's personal information is encrypted with the common key created, the common key is encrypted with the public key of the authentication server 3, which the user set, and the public key of the authentication server 3 is directly set by the user in the finger print acquisition apparatus 7. Hence, there is such an effect that it is possible to securely protect the user's personal privacy, which is the finger print information that is the biometrics information, in a style of reflecting user's intention since the finger print information is transferred over the network in such a condition that only the authentication server 3, which the user assigned, can decode the finger print information. Furthermore, a user can instruct only a public key of the authentication server 3 with a floppy disk, a magnetic card, an IC card, or key entry to the finger print acquisition apparatus 7, there is no problem on security even if the floppy disk, magnetic card, or IC card is lost or stolen, which saves this public key, and the user can receive the personal authentication with a substitute, which saves the same public key or the same article. There is another effect that it is unnecessary to perform processing such as special notification and reissue at the time of loss and burglar and it is possible to lighten the administration load.

[0039] In addition, since the data and time, when the authentication information was created, is confirmed in the authentication server 3, it is possible to prevent reuse of the invalid authentication information, and to keep security high since it can be confirmed in the Web server 4 in the authentication-requester's side whether the authentication is performed by the authentication information authentication server 3.

[0040] Although the present invention is applied in the Web system 1 in this embodiment, the same effect can be obtained even if the Web server S/W 4C and browser 5A are other applications, constructing another system, such as accounting information administration server S/W and accounting information administration client S/W, and database retrieval server S/W and database retrieval client S/W.

Embodiment 2.

[0041] This embodiment is obtained by simplifying the first embodiment, and the Web server 4 and user terminal 5 in Fig. 1 become only a user terminals 5 in Fig. 3. Since, in Fig. 3 where the same symbols are assigned to the parts corresponding to the parts in Fig. 1, applications for which the personal authentication is necessary present in only the user terminal 5, the Web server S/W 4C and two applications, constructing the browser 5A,

that are shown in Fig. 1 are replaced to database retrieval S/W 5E, and the Web server database 4A is replaced to a local database 5C. In this case, the authentication request unit 4B and encryption processing unit 4D that construct the Web server 4 in Fig. 1 become a component of the user terminal 5 in Fig. 3.

[0042] In the second embodiment, the user terminal 5 is a computer system such as a personal computer and a workstation, where the local database 5C, an encryption processing unit 5F, a authentication request unit 5D, a database retrieval S/W 5E that is an application for which the personal authentication is required, and authentication information acquisition S/W 5B operate. In addition, a biometrics acquisition apparatus 6 is connected to the user terminal 5, and has the same configuration as that in the first embodiment. Furthermore, the authentication server 3 also has the same configuration as that in the first embodiment described above.

[0043] Here, a case that a finger print acquisition apparatus 7 is used as the biometrics acquisition apparatus 6 will be exemplified.

[0044] Next, operation will be described.

[0045] Fundamentally, this is similar to that in the first embodiment, and in Fig. 4 where the same symbols are assigned to the parts corresponding to those in Fig. 2, first, a case that a user accesses information in the local database 5C, which has high confidentiality, with the database retrieval S/W 5E that is an application operating in the user terminal 5 will be described. The database retrieval S/W 5E that is an application performing access control of the information having high confidentiality is required to perform the user authentication so as to judge whether the user has access authorization (SP5).

[0046] The authentication information acquisition S/W 5B in the user terminal 5 acquires the finger print information, which is necessary for the authentication, from the finger print information acquisition apparatus 7 (SP6). At this time, this S/W 5B may cooperate with other S/W (software such as a driver acquiring the authentication information).

[0047] The authentication information acquisition unit 7A in the finger print acquisition apparatus, which is instructed to acquire the finger print information from the authentication information acquisition S/W 5B in the user terminal 5 acquires the finger print information from the user (SP1). Although encryption processing unit 7B encrypts this finger print information since this finger print information is user's personal information, first, the encryption processing unit 7B creates a common key in the common key encryption method for encrypting this finger print information, and encrypts the finger print information with this common key. At the same time, the encryption processing unit 7B acquires date and time information, creates a message digest with connecting the date and time information with the common key, and further encrypts the message digest with the common key (SP2).

[0048] The public key acquisition unit 7C in the finger print acquisition apparatus 7 acquires the public key of the authentication server 3 from user's instruction such as a floppy disk, a magnetic card, an IC card, or key entry. Alternatively, if the finger print acquisition apparatus 7 is properly administrated, the public key of the authentication server 3 is fixedly saved in the public key acquisition unit 7C in the finger print acquisition apparatus 7, and hence the user may use the public key after recognizing the public key. Next, the encryption processing unit 7B encrypts the common key with the public key of the authentication server 3 (SP3). Then, the finger print acquisition unit 7A transfers the finger print information encrypted, the date and time information, the message digest with connecting the date and time information with the common key that is encrypted, and the encrypted common key as the authentication information to the authentication information acquisition S/W 5B in the user terminal 5 (SP4).

[0049] The authentication information acquisition S/W 5B in the user terminal 5 acquires a user ID such as a user name and a mail and adds them to the authentication information (SP7).

[0050] The authentication request unit 5D transfers this authentication information to the authentication controller 3A in the authentication server 3 (SP7).

[0051] The authentication controller 3A in the authentication server 3 makes the encryption processing unit 3C decode the authentication information transferred, and performs the user authentication. At this time, the encryption processing unit 3C compares the message digest created from the date and time information and common key, which is transferred, in the authentication server 3 with the message digest decoded from the message digest obtained by connecting the date and time information, which is encrypted, with the common key, and confirms the validity of the date and time, when the authentication information was created, in consideration of transfer delay (SP12).

[0052] The authentication controller 3A performs finger print matching from the finger print information and user ID, which are included in the authentication information transferred, and personal information originally saved in the authentication information database 3B in the authentication server 3. The authentication controller 3A creates the result of the authentication showing that the user is valid if the authentication controller 3A identifies the user as the principal in consequence of matching, or judges that the user is not the principal if the authentication controller 3A cannot identify the user as the principal in consequence of the matching, and creates the result of the authentication. This result of the authentication is delivered to the encryption processing unit 3C, and the encryption processing unit 3C creates a message digest of the result of the authentication, encrypts the message digest with the secret key of the authentication server 3, that is, performs digital signature, and delivers this message digest, which is

encrypted, to the authentication controller 3A. The authentication controller 3A informs the authentication request unit 5D in the user terminal 5 of the result of the authentication with including the message digest, which is encrypted, in the result of the authentication (SP13).

[0053] The authentication request unit 5D in the user terminal 5 that receiving the result of the authentication informs the encryption processing unit 5F of the result of the authentication. The encryption processing unit 5F decodes the informed message digest, which is encrypted, with the public key of the authentication server 3, and confirms that the message digest is surely the valid message from the authentication server 3 by comparing the decoded message digest with the message digest of the informed result of the authentication (SP10). If the authentication request unit 5D receives from the encryption processing unit 5D the result of confirmation that the information is the valid information from the authentication server 3, the authentication request unit 5D informs the database retrieval S/W 5E of the result of the authentication. The database retrieval S/W 5E judges approval or disapproval of access to the information in the local database 5C, which has high confidentiality, to the user according to the result of the authentication. For example, the database retrieval S/W 5E performs operation to, the user access such as the display of the confidential information (SP11).

[0054] According to this configuration, when the user terminal 5 requests the authentication server 3 to perform the personal authentication, it is possible to obtain the same effects as those in the first embodiment.

[0055] Although the present invention is applied in the database retrieval system 1 in this embodiment, the same effects can be obtained even if the database retrieval S/W is an application, constructing another system, such as accounting information administration S/W.

Embodiment 3.

[0056] This third embodiment is an embodiment where the encryption processing unit 7B and public key acquisition unit 7C in the finger print acquisition apparatus 7 that is a biometrics acquisition apparatus 6 in the first embodiment present in the user terminal 5.

[0057] In Fig. 5 where the same symbols are assigned to the parts corresponding to those in Fig. 1, the user terminal 5 is a computer system such as a personal computer and a workstation, where a browser 5A displaying the information of the Web server terminal 4, an encryption processing unit 5F encrypting the finger print information, a public key acquisition unit 5G acquiring the public key of the authentication server 3, and an authentication information acquisition S/W 5B operate. In addition, a biometrics acquisition apparatus 6 is connected to the user terminal 5. Furthermore, the authentication server 3 and Web server 4 have the same

configuration as that in the first embodiment.

[0058] In addition, the biometrics information which the biometrics acquisition apparatus 6 in this embodiment acquires can be image data, image data that is not processed such as electrostatic data, and also characteristic point data obtained by extracting characteristics from image data. The biometrics acquisition apparatus 6 can be a simple device that only acquires image data and does not have a CPU. Here, a case that the finger print acquisition apparatus 7 is used as the biometrics acquisition apparatus 6 will be exemplified.

[0059] The finger print acquisition apparatus 7 is composed of a finger print information acquisition unit 7A that acquires the finger print information by performing image processing and the like and transfers the finger print information to the user terminal.

[0060] Next, operation will be described.

[0061] Fundamentally, the operation is the same as that in the first embodiment, in Fig. 6 where the same symbols are assigned to the parts corresponding to those in Fig. 2, first, a case that a user accesses the information in the Web server database 4A, which has high confidentiality, in the Web server 4 with the browser 5A that is an application operating in the user terminal 5 will be described (SP5). The Web server S/W 4C, which is an application performing access control of the information having high confidentiality, is required to perform the user authentication so as to judge whether the user has an access authority.

[0062] The authentication information acquisition S/W 5B in the user terminal 5 acquires the finger print information, which is biometrics information necessary for the authentication, from the finger print acquisition apparatus 7 (SP6). At this time, the S/W 4C may operate with cooperating with other S/W (software such as a driver acquiring the authentication information).

[0063] The finger print information acquisition unit 7A in the finger print acquisition apparatus 7 which is instructed to acquire the finger print information by the authentication information acquisition S/W 5B in the user terminal 5 acquires the finger print information from the user (SP1), and transfers the finger print information to the authentication information acquisition S/W 5B in the user terminal 5 (Sp4).

[0064] The authentication information acquisition S/W 5B in the user terminal 5 makes the encryption processing unit 5F encrypt this finger print information since this finger print information is user's inherent personal information. First, the encryption processing unit 5F creates a common key in the common key method for encrypting this finger print information, and encrypts the finger print information with this common key. At the same time, the encryption processing unit 5F acquires date and time information, creates a message digest with connecting the date and time information with the common key, and further encrypts the message digest with the common key (SP2).

[0065] The public key acquisition unit 5G in the user

terminal 5 acquires a public key of the authentication server from user's instruction such as a floppy disk, a magnetic card, an IC card, or key entry.

[0066] Next, the encryption processing unit 5F encrypts the common key with the public key of the authentication server 3 (SP3). Then, the authentication information acquisition S/W 5B transfers the finger print information encrypted, the date and time information, the message digest with connecting the date and time information with the common key that is encrypted, and the encrypted common key, the acquired authentication information as the authentication information to the Web server 4 through the browser 5A. At this time, the browser 5A transfers the authentication information with adding a user ID such as a user name and a mail address, which the browser 5A acquires separately, to the authentication information (SP7).

[0067] The authentication request unit 4B in the Web server 4 transfers the authentication information, which the authentication request unit 4B acquires, to the authentication controller 3A in the authentication server 3 through the Web server S/W 4C (SP9).

[0068] The authentication controller 3A in the authentication server 3 makes the encryption processing unit 3C decode the authentication information transferred, and performs the user authentication. At this time, the encryption processing unit 3C compares the message digest created from the date and time information and common key, which are transferred, in the authentication server 3 with the message digest decoded from the message digest obtained by connecting the date and time information, which is encrypted, with the common key, and confirms the validity of the date and time, when the authentication information was created, in consideration of transfer delay (SP12).

[0069] The authentication controller 3A performs finger print matching from the finger print information and user ID, which are included in the authentication information transferred, and personal information originally saved in the authentication information database 3B in the authentication server 3. The authentication controller 3A creates the result of the authentication showing that the user is valid if the authentication controller 3A identifies the user as the principal in consequence of matching, or judges that the user is not the principal if the authentication controller 3A cannot identify the user as the principal in consequence of the matching, and creates the result of the authentication. The result of this authentication is delivered to the encryption processing unit 3C, and the encryption processing unit 3C creates a message digest of the result of the authentication, encrypts the message digest with the secret key of the authentication server 3, that is, performs digital signature, and delivers this message digest, which is encrypted, to the authentication controller 3A. The authentication controller 3A informs the authentication request unit 4B in the Web server 4 of the result of the authentication with including the message digest, which

is encrypted, in the result of the authentication (SP13).

[0070] The authentication request unit 4B in the Web server 4 receiving the result of the authentication informs the encryption processing unit 4D of the result of the authentication. The encryption processing unit 4D decodes the informed message digest, which is encrypted, with the public key of the authentication server 3, and confirms that the message digest is surely the valid message from the authentication server 3 by comparing the decoded message digest with the message digest of the informed result of the authentication (SP10). If the authentication request unit 4B is informed from the encryption processing unit 5D that it was confirmed that the information was the valid information from the authentication server 3, the authentication request unit 4B informs the Web server S/W 4C of the result of the authentication. The Web server S/W 4C judges approval or disapproval of access to the information in the Web server database 4A, which has high confidentiality, to the user according to the result of the authentication. For example, the Web server S/W 4C performs operation to the user access such as the display of the confidential information (SP11).

[0071] In this manner, the finger print information that is user's personal information is encrypted with the common key created, the common key is encrypted with the public key of the authentication server 3, which the user set, and the public key of the authentication server 3 is directly set by the user in the user terminal 5. Hence, there is such an effect that it is possible to securely protect the user's personal privacy, which is the finger print information that is the biometrics information, in a style of reflecting user's intention since the finger print information is transferred over the network in such a condition that only the authentication server 3, which the user assigned, can decode the finger print information. Nevertheless, although security becomes low in comparison with a case that the finger print information is encrypted from the finger print acquisition apparatus 7 since there arises a period, when the finger print information exists in the user terminal 5 without being encrypted, there is no problem if the user terminal 5 itself is properly administrated, and there is an effect that the configuration of the finger print acquisition apparatus 7 becomes simple since the encryption processing unit and public key acquisition unit are unnecessary in the finger print acquisition apparatus 7. As effects except the above-described effects, the similar effects as those in the first embodiment can be obtained. In addition, this embodiment can be applied also to the application such as the database retrieval S/W 5E, which are shown in the second embodiment, and hence it is possible to obtain the same effects.

[0072] Furthermore, in all of the first, second, and third embodiments, a common key for encrypting the user's biometrics information obtained is created. Nevertheless, it is necessary to eliminate the tendency of the random numbers for creating the common key so as to

make it difficult to break the common key. Since the biometrics information generally has values different every acquisition, the message digest of the biometrics information acquired is used as a part or all of the random numbers.

[0073] As described above, it is simply performed to eliminate the tendency of the generated random numbers since the random numbers generated from the message digest of the biometrics information acquired are generated. Furthermore, since a part or all of this random numbers are used as the random numbers for generating the common key, it is possible to generate the random numbers irrelevant to the number of authentication times and the time and to construct a system that is strong on security against the decoding of the common key.

Embodiment 4.

[0074] Although only the valid administrator can perform the administration of the biometrics information acquisition apparatus, it is necessary that the administrator, being not authenticated, or another person acting for the administrator can perform initialization of a biometrics acquisition apparatus if there arises such a state that no one cannot authenticate the valid administrator. This case will be described with exemplifying such a case that, in the finger print acquisition apparatus in the first and second embodiments, the finger print acquisition apparatus is properly administrated and a public key of an authentication server is fixedly determined in the finger print acquisition apparatus.

[0075] Fig. 7 is the configuration at the time of administrating, that is, setting and changing the public key fixedly saved in a public key acquisition unit 12C in a finger print acquisition apparatus 12. An administration terminal 11 is a computer system such as a personal computer and a workstation, where an administration S/W 11A operates. The finger print acquisition apparatus 12 is composed of a finger print information acquisition unit 12A and an encryption processing unit 12B, a public key acquisition unit 12C, and an administration unit 12D.

[0076] The administration S/W 11A in the administration terminal 11 issues authentication request of an administrator to the finger print acquisition apparatus 12 so as to execute setting of the public key. Although an administrator authentication unit 12D1 in an administration unit 12D in the finger print acquisition apparatus 12 acquires administrator's finger print from the finger print information acquisition unit 7A and performs finger print matching of the administrator, the administrator authentication unit 12D1 may become in such a condition that the unit 12D1 cannot identify the administrator as the valid administrator. This corresponds to a case that the finger print itself is lost due to an injury of the administrator. In this case, although the administration S/W 11A instructs an initializer authentication unit 12D2 in the administration unit 12D in the finger print acquisition

apparatus 12 to perform initialization, the S/W 11A performs the authentication of the initializer with means, being set beforehand, such as a password. The initializer authentication unit 12D2 performs only the authentication of the initializer, only the initialization of the finger print acquisition apparatus is executed by the authentication of the initializer authentication unit 12D2.

[0077] In this manner, by providing the authentication means for an initializer separately from an ordinary administrator, there are such effects that it is possible to perform only the initialization if an administrator cannot be authenticated and suddenly becomes absent, and furthermore to prevent a person not having the initialization authority from invalidly performing the initialization.

Embodiment 5.

[0078] Fig. 8 shows an authentication server where means for finding invalid authentication is applied to the above-described authentication server so as to enhance reliability. An authentication server 13 is a computer system such as a personal computer and a workstation, which is composed of a logging unit 13D, an authentication controller 13A, an encryption processing unit 13C, and an authentication information database 13B.

[0079] The logging unit 13D in the authentication server 13 logs a matching rate that is the result of matching biometrics at the time of the user authentication. In addition, the logging unit 13D confirm that a matching rate at this time does not change more than or equal to a preset value determined by the administrator by comparing the matching rate at this time with the average matching rate at the time of identifying a user as the principal until the previous occasion if the authentication controller 13A does not identifies the user as the principal at the time of the user authentication. If the matching rate changes more than or equal to a fixed value, the logging unit 13D increases the number of failure times. If the number of failure times reaches the value more than or equal to a fixed value determined by the administrator, the logging unit 13D informs the administrator, who is registered beforehand, and the user herself/himself of the failure.

[0080] Since this structure informs the administrator and the user, who is personated, of the abnormal result of the matching that is unique in biometrics authentication, it is possible to early find the invalid authentication and to keep the high security of the system.

[0081] In addition, since biometrics information becomes information different every acquisition even if matching rates are the same, it is stochastically very small that biometrics information acquired in the past coincides with the new biometrics information. An invalidity-finding structure using this characteristic of the biometrics authentication will be described.

[0082] The logging unit 13D in the authentication server 13 that is shown in Fig. 8 compares a matching

rate at this time with the matching rate at the time of identifying a user as the principal until the previous occasion and confirms that both matching rates are the same if the authentication controller 13A identifies the user as the principal at the time of the user authentication. If the matching rates are the same and a message digest of the biometrics information is not saved, the logging unit 13D informs the authentication controller 13A of making the user authentication unsuccessful, and the authentication controller 13A makes the result of the authentication unsuccessful. At the same time, the logging unit 13D saves the message digest of the biometrics information with the matching rate. If the matching rates are the same and the message digest of the biometrics information is saved, the logging unit 13D calculates a message digest of the biometrics information at this time, compares this message digest with the message digest of the biometrics information at the same matching rate in the past. If both message digest are different from each other, the logging unit 13D identifies the user as the principal, but, if both coincide with each other, the logging unit 13D informs the authentication controller 13A of making the user authentication unsuccessful since there is a possibility of masquerade. The authentication controller 13A makes the result of the authentication unsuccessful. The logging unit 13D increases the number of failure times at the same matching rate if the authentication is made unsuccessful due to coincidence of the matching rate and message digest, and, if this number of failure times reaches a value more than or equal to the fixed value determined by the administrator, the logging unit 13D informs the administrator and the user herself/himself that are registered beforehand.

[0083] Since this structure informs the administrator and the user, who is personated, of such an abnormal state that it is considered to be the masquerade caused by leakage of the biometrics information, it is possible to early find the invalid authentication and to keep the high security of the system. In addition, there are such effects that it is possible to reduce a storage area since an object which the logging unit 13D saves is the message digest of the biometrics information at the time of the same matching rate after the second occasion, and that it is possible to shorten the time consumed for comparison in comparison with the comparison, performed by using biometrics information itself, because of the comparison performed by using the message digests.

[0084] As described above, according to the present invention, there is such an effect that it is possible to securely protect the user's personal privacy, which is the finger print information that is the biometrics information, in a style of reflecting user's intention since the finger print information is transferred over the network in such a condition that only the authentication server, which the user assigned, can decode the finger print information, and it is possible to prevent invalid authentication information from being reused since the date

and time when the authentication information was created can be confirmed in the authentication server 3, and to keep the security of the system high since the authentication request side can confirm whether the user is authenticated by the authentication server.

[0085] Furthermore, although a user can instruct a public key of the authentication server, there is no problem on security even if the floppy disk, magnetic card, or IC card, which saves this public key, is lost or stolen, and the user can receive the personal authentication with a substitute, which saves the same public key or the same article. There is another effect that it is unnecessary to perform processing such as special notification and reissue at the time of loss and burglar and it is possible to lighten the administration load.

[0086] In addition, since the present invention creates random numbers, used for creating the common key, from the biometrics information acquired, it is possible to generate the random numbers irrelevant to the number of authentication times and the time, and to construct a system that is strong on security against the decoding of the common key.

[0087] Furthermore, by providing the authentication means for an initializer separately from an ordinary administrator, there are such effects that it is possible to perform the initialization even if an administrator suddenly becomes absent, and furthermore to prevent a person not having the initialization authority from invalidly performing the initialization.

[0088] Moreover, since the authentication server logs at the time of the user authentication and informs a person, who is registered beforehand, of the abnormal result of the matching that is unique in biometrics authentication, it is possible to early find the invalid authentication and to keep the high security of the system.

Claims

1. A remote authentication system in which an authentication server 3, an application server 4, and a user terminal 5 are connected to a network 2 respectively, and which authenticates a user using the user terminal, wherein the authentication server has a pair of a public key and a secret key in a public key encryption method, announces the public key, and conceals the secret key; wherein at least one kind or a plural kind of biometrics acquisition apparatus 6 is connected to the user terminal; wherein the biometrics acquisition apparatus: encrypts user's biometrics information, acquired at the time of authentication, with a common key in a common key encryption method; acquires date and time information, creates a message digest with connecting the date and time information with the common key, and further encrypts the message digest with the common key; acquires the public

key of the authentication server, which the user assigns, and encrypts the common key with the public key of the authentication server; and transfers the biometrics information encrypted, the common key and date and time information, which is encrypted, and the message digest encrypted with connecting the date and time information with the common key, as authentication information to the user terminal;

wherein the user terminal and the application server transfer the authentication information to the authentication server; and

wherein the authentication server: decodes user's biometrics information with the common key acquired by decoding the authentication information, which is transferred, with the secret key; authenticates the user with the biometrics information; encrypts result of authentication and a message digest of the result of the authentication; and transfers both to the application server.

2. A remote authentication system in which an authentication server 3, an application server 4, and a user terminal 5 are connected to a network 2 respectively, and which authenticates a user using the user terminal, wherein the authentication server has a pair of a public key and a secret key in a public key encryption method, announces the public key, and conceals the secret key, and at least one kind or a plural kind of biometrics acquisition apparatus 6 is connected to the user terminal; wherein the biometrics acquisition apparatus: encrypts user's biometrics information, acquired at the time of authentication, with a common key in a common key encryption method; acquires date and time information, creates a message digest with connecting the date and time information with the common key, further encrypts the message digest with the common key; acquires the public key of the authentication server, which the user assigns; encrypts the common key with the public key of the authentication server; and transfers the biometrics information encrypted, the common key and date and time information, which is encrypted, and the message digest encrypted with connecting the date and time information with the common key, as authentication information to the user terminal; wherein the user terminal transfers the authentication information to the authentication server; and wherein the authentication server: decodes user's biometrics information with the common key acquired by decoding the authentication information, which is transferred, with the secret key; authenticates the user with the biometrics information; encrypts result of authentication and a message digest of the result of the authentication with the secret key; and transfers both to the user terminal.

3. The remote authentication system according to any one of claims 1 and 2, wherein the biometrics acquisition apparatus transfers biometrics information to the user terminal without encrypting the biometrics information at the time of authentication; and wherein the user terminal: encrypts the user's biometrics information, which is obtained, with a common key in a common key encryption method; acquires a public key of a authentication server that a user assigns; encrypts the common key with the public key of the authentication server; acquires date and time information, creates a message digest with connecting the date and time information with the common key, encrypts the message digest with the common key; and transfers the biometrics information encrypted, the common key and date and time information, which is encrypted, and the message digest encrypted with connecting the date and time information with the common key, as authentication information to the user terminal.
4. The remote authentication system according to any one of claims 1 to 3, wherein the user terminal uses biometrics information as a part or all of random numbers for creating the common key when, at the time of authentication, the user terminal creates the common key in a common key encryption method for encrypting the user's biometrics information acquired.
5. The remote authentication system according to any one of claims 1 to 3, wherein the biometrics acquisition apparatus includes an authentication unit of an administrator administrating the biometrics acquisition apparatus and an authentication unit of an initializer initializing the biometrics acquisition apparatus; and wherein the two authentication units perform authentication separately, and performs initialization with authentication of the initializer even if the administrator is not authenticated.
6. The remote authentication system according to any one of claims 1 to 3, wherein the authentication server: saves a historic record of a matching rate that is result of matching biometrics at the time of user authentication; compares a matching rate with an average matching rate at the time of identifying a user as a principal until the previous occasion if the authentication server does not identify the user as the principal at the time of user authentication; confirms whether a matching rate at this time changes more largely than a preset value determined by an administrator; and informs a contact, who is registered beforehand, if a number of failed times due to changes more largely than a fixed value reaches a fixed value determined by the

administrator.

- 7. The remote authentication system according to any one of claims 1 to 3, wherein the authentication server: saves historic records of matching rates that are results of matching biometrics at the time of user authentication; compares a matching rate with a matching rate at the time of identifying a user as a principal until the previous occasion at the time of user authentication if the authentication server identifies the user as the principal; makes the user authentication unsuccessful if the two matching rates are the same rates and a message digest of biometrics information is not saved, performs message digest calculation of biometrics information at this time, saves the message digest of biometrics information with the matching rate; saves a message digest of biometrics information at this time with a matching rate as a pair with calculating the message digest of biometrics information at this time if the two matching rates are the same and a message digest is saved, compares the message digest of biometrics information at this time with the message digest of biometrics information at the same matching rate in the past, identifies the user as a principal if both message digests are different from each other; does not identify the user as a principal if a pair of a matching rate and a message digest at this time completely coincides with a pair of a matching rate and a message digest in the past; and informs a contact, who is registered beforehand, if a number of cases that the pair of the matching rate and message digest at this time completely coincides with the pair of the matching rate and message digest in the past reaches a value equal to or more than a fixed value which is determined by an administrator.

5

10

15

20

25

30

35

40

45

50

55

FIG. 1

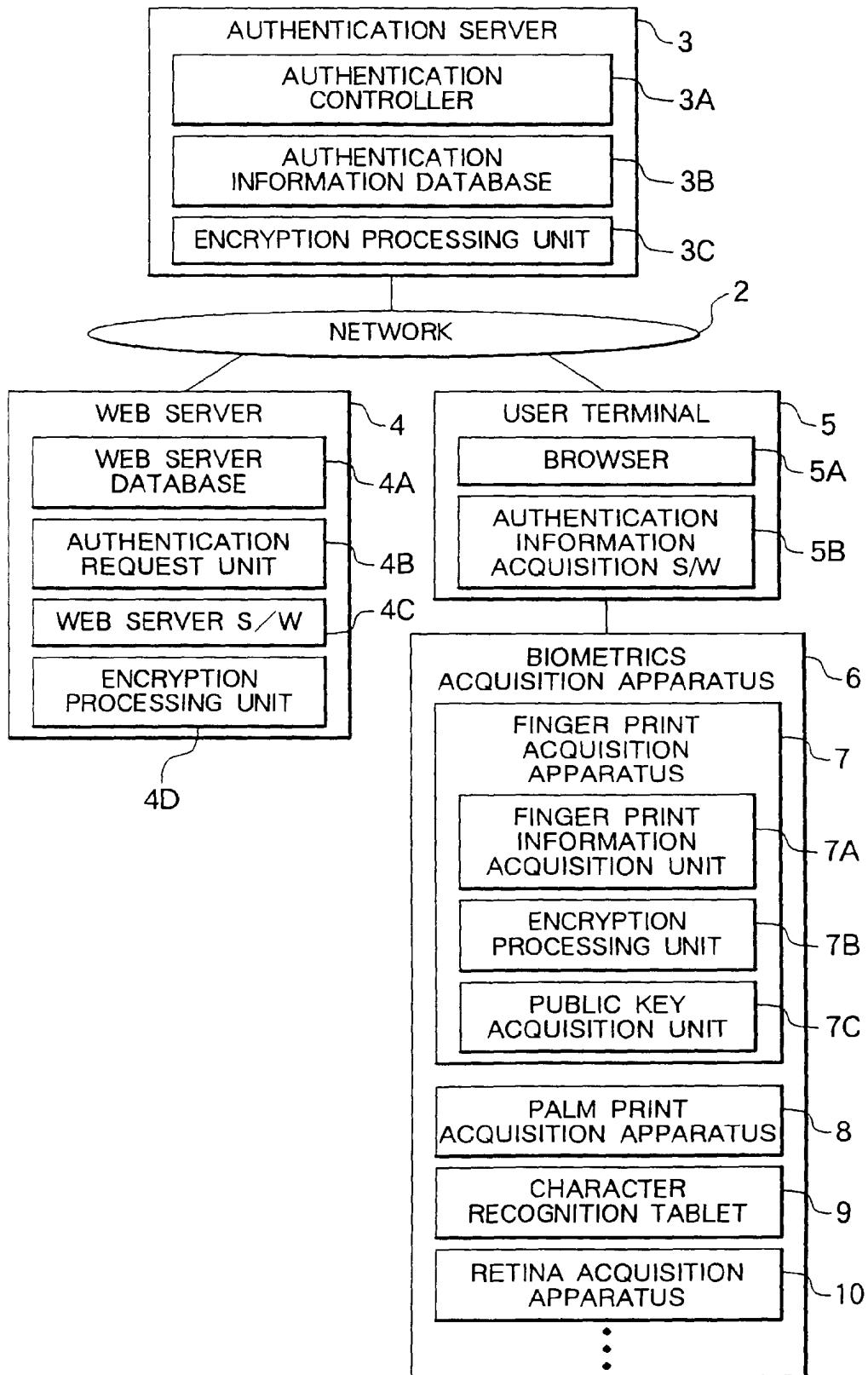


FIG. 2

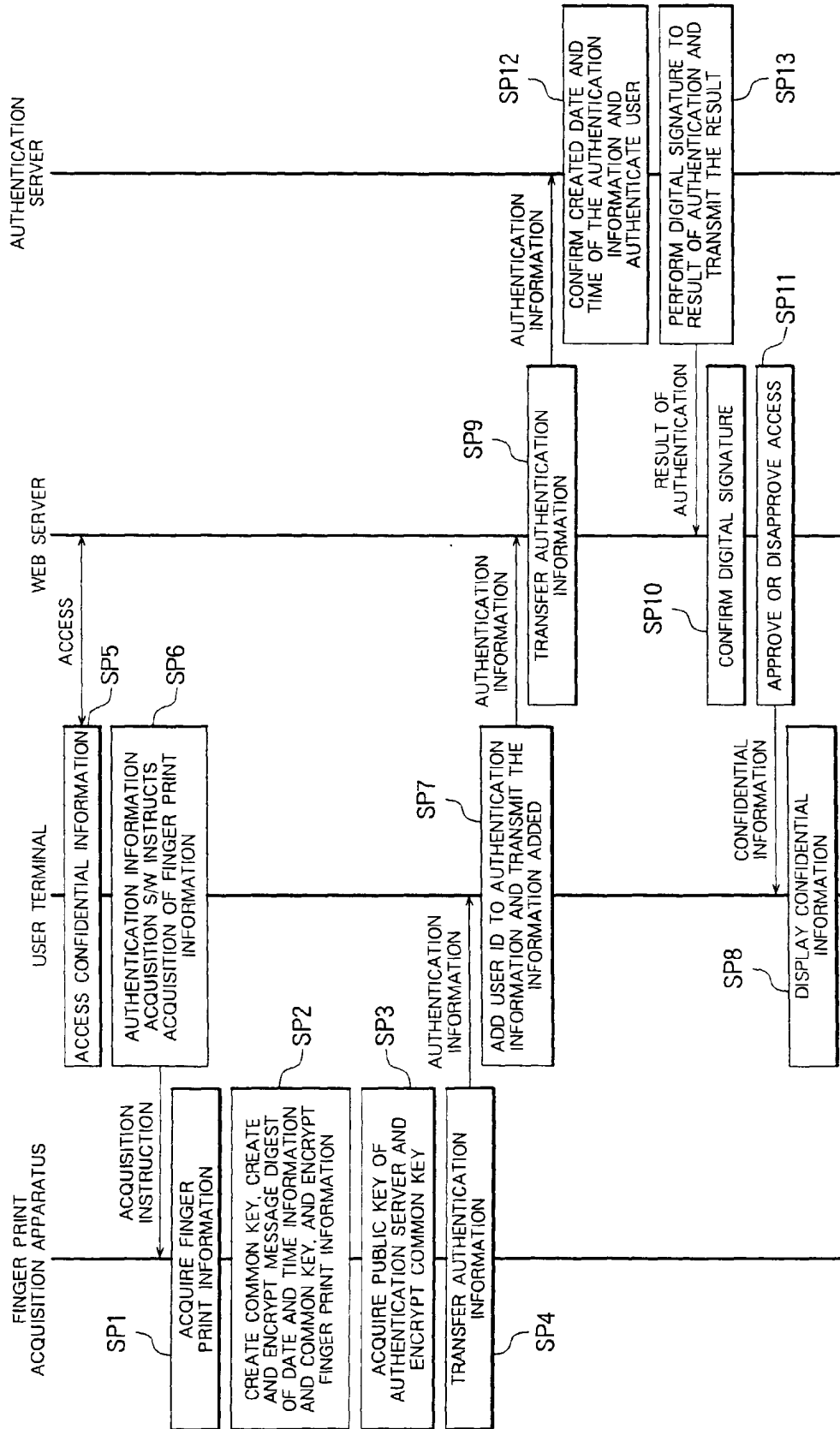


FIG. 3

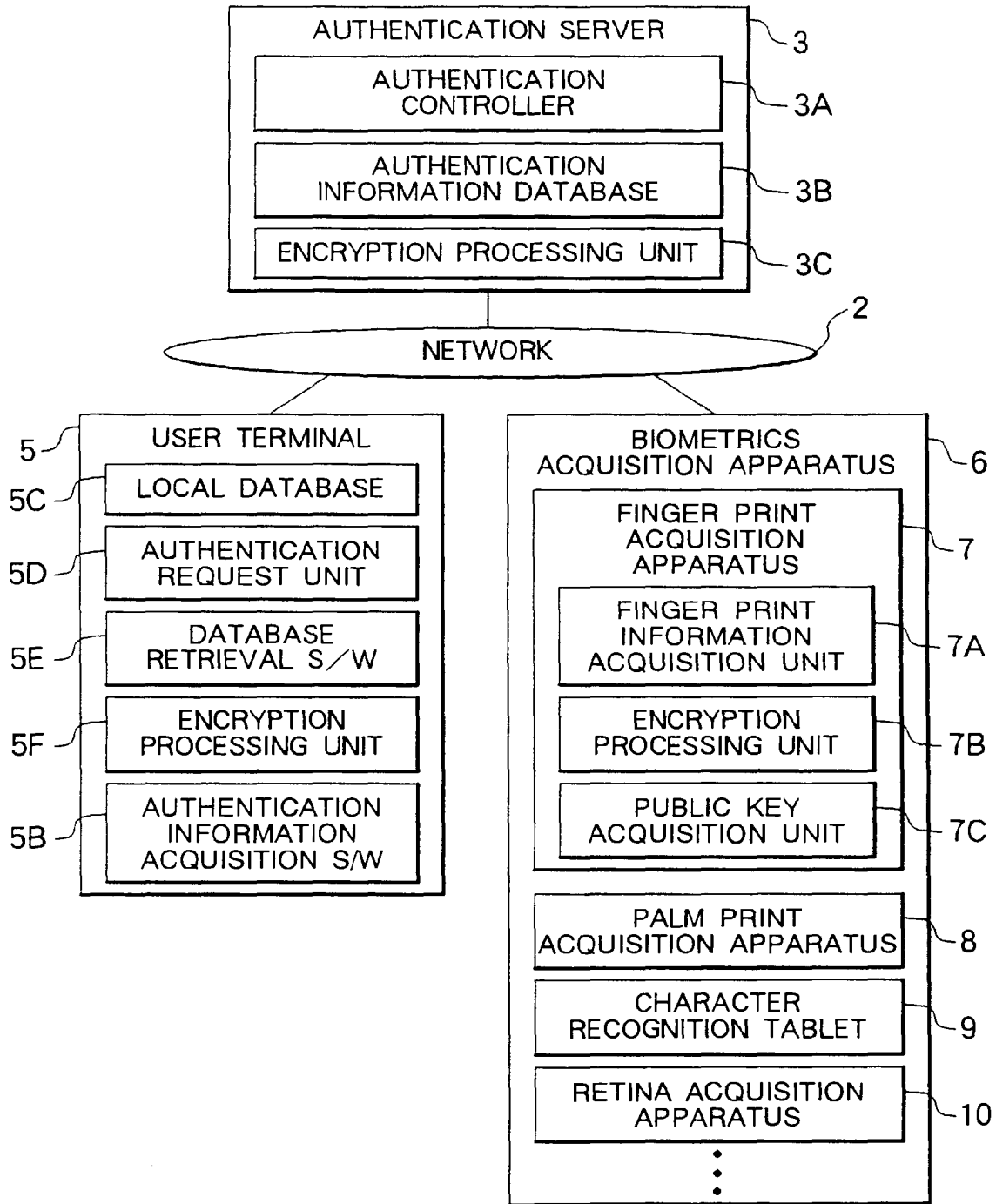


FIG. 4

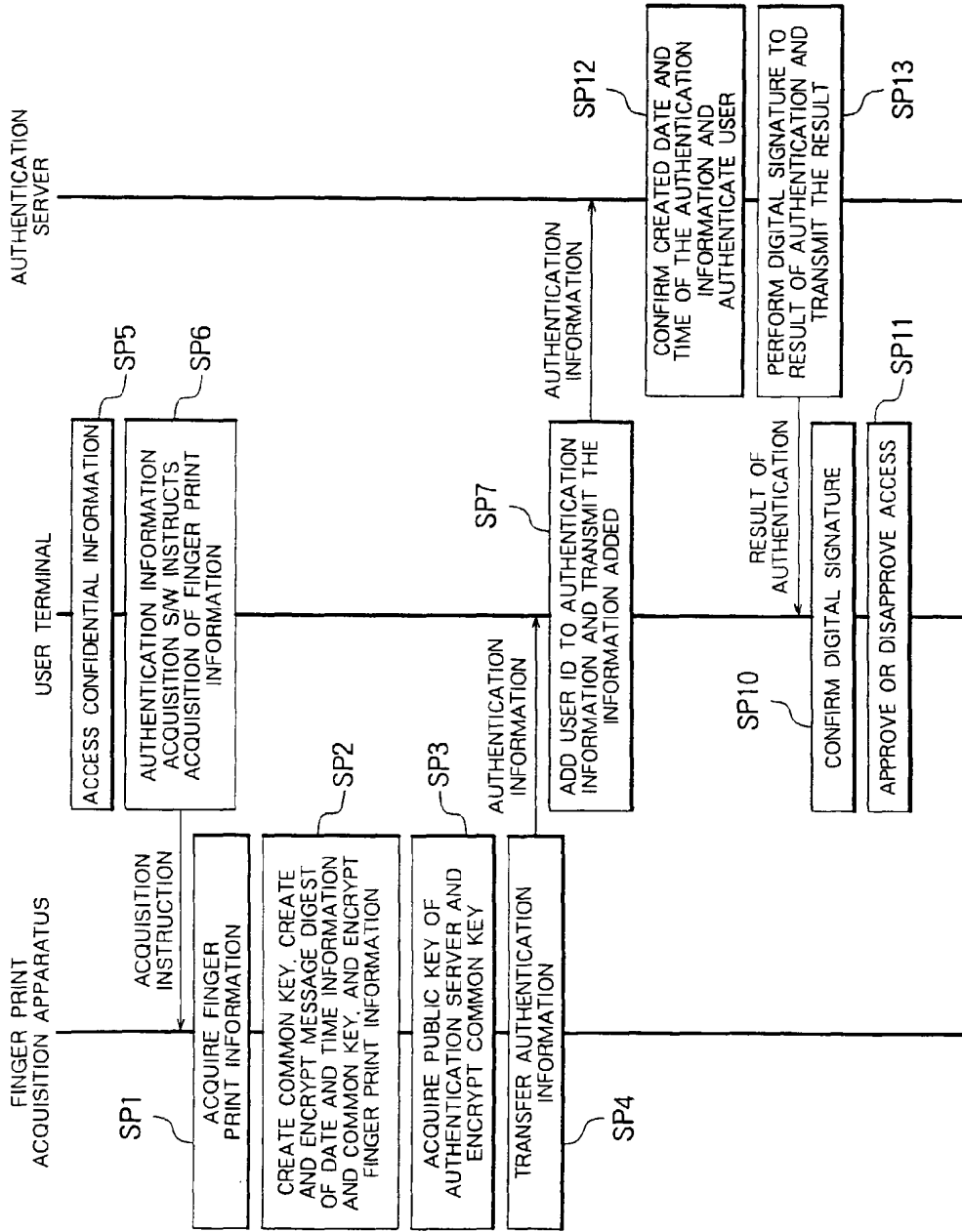


FIG. 5

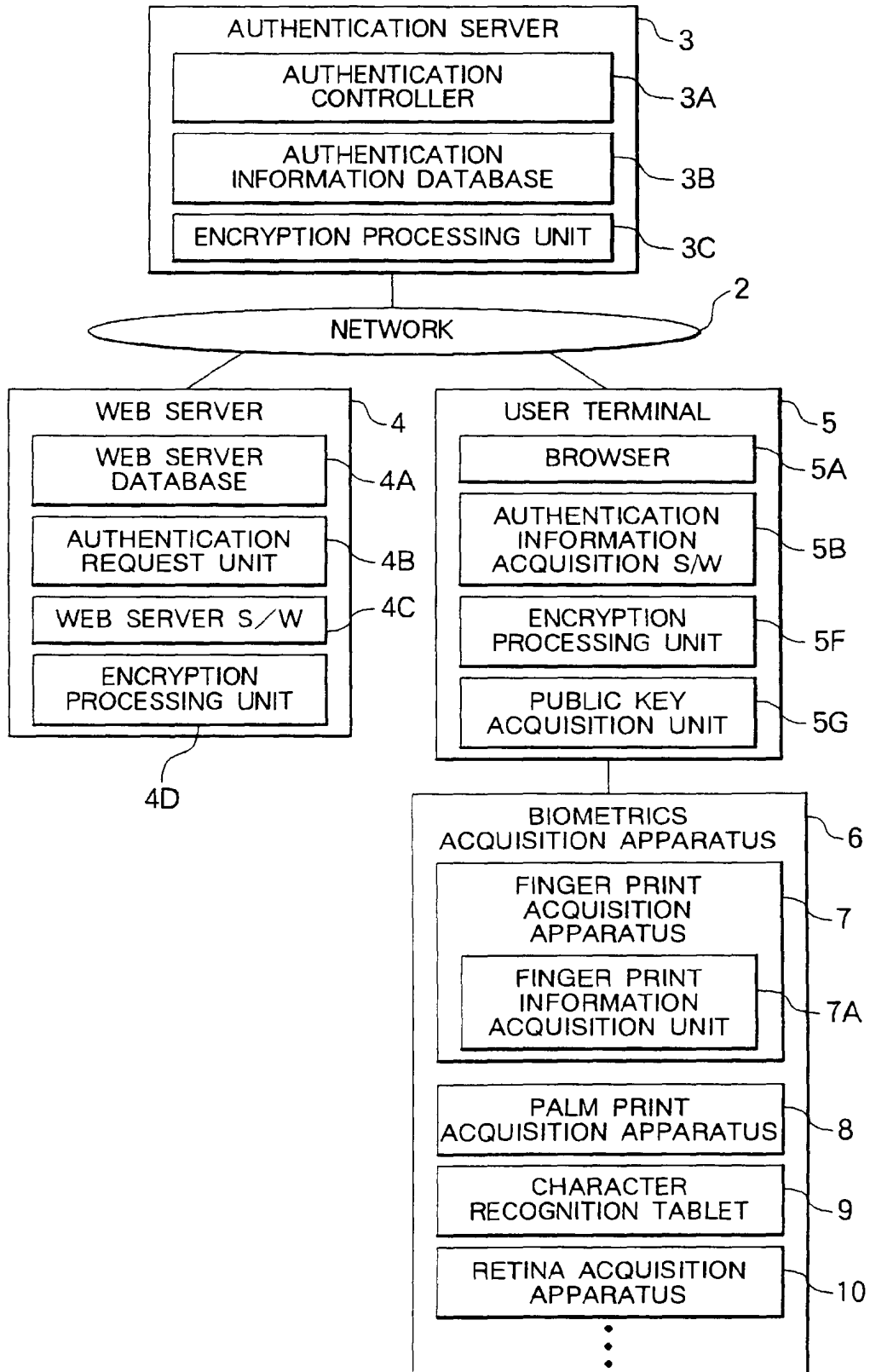


FIG. 6

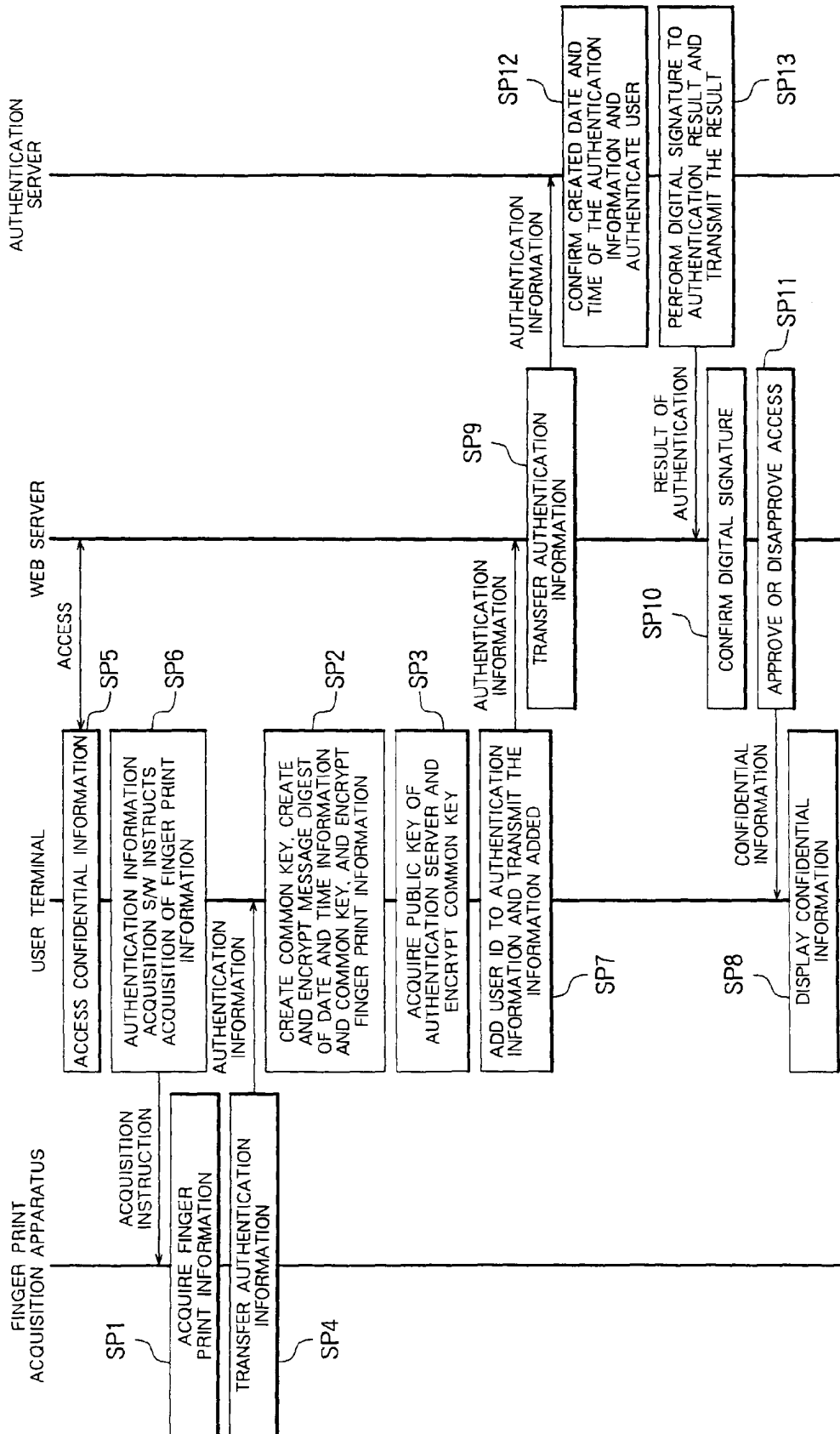


FIG. 7

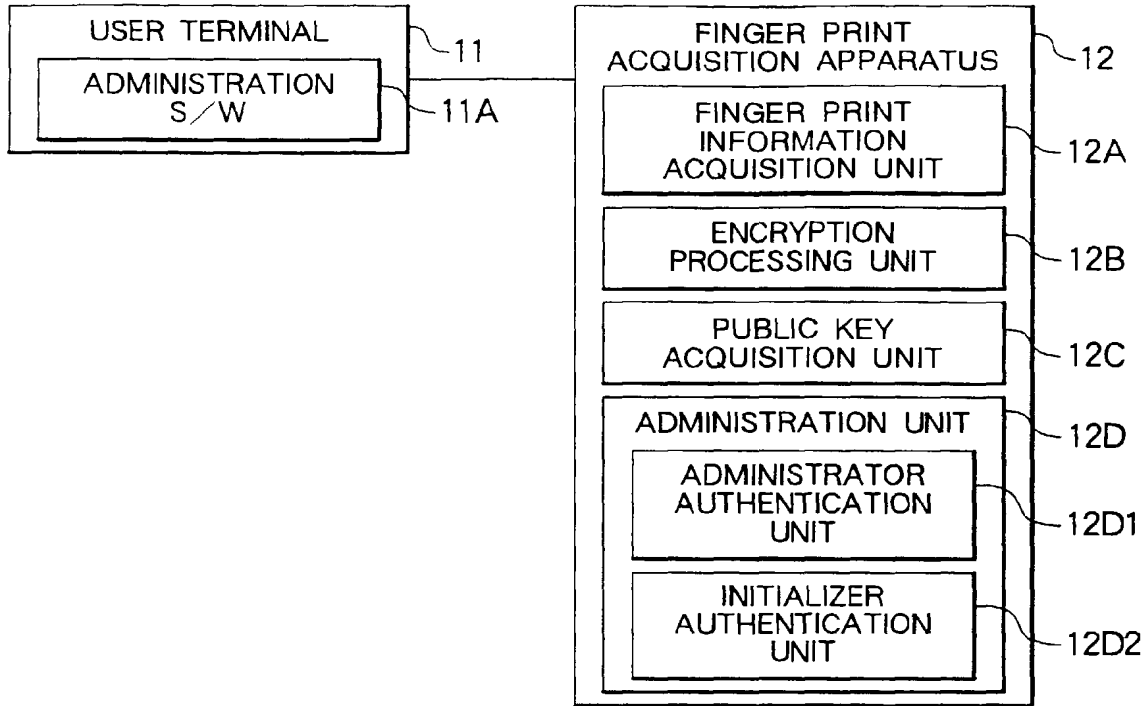
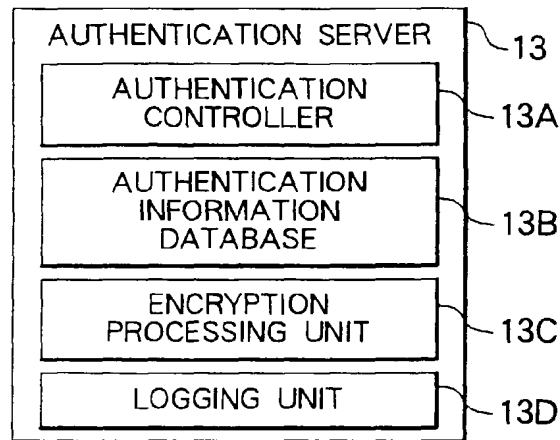


FIG. 8



Electronic Patent Application Fee Transmittal

Application Number:	11768729
Filing Date:	26-Jun-2007
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Filer:	Matthew H. Grady
Attorney Docket Number:	W0537-700620

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
RCE - 2nd and Subsequent Request	2820	1	850	850
Total in USD (\$)				850

Electronic Acknowledgement Receipt

EFS ID:	18608686
Application Number:	11768729
International Application Number:	
Confirmation Number:	3536
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Customer Number:	37462
Filer:	Matthew H. Grady
Filer Authorized By:	
Attorney Docket Number:	W0537-700620
Receipt Date:	28-MAR-2014
Filing Date:	26-JUN-2007
Time Stamp:	10:26:26
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$850
RAM confirmation Number	10302
Deposit Account	502762
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Transmittal Letter	Information_Disclosure_Statement.pdf	21816 53da5c394a4e6ae19a8e79976108264d54214bf8	no	2
Warnings:					
Information:					
2	Request for Continued Examination (RCE)	Request_for_Continued_Examination_Fillable_PDF.PDF	697529 c653e2b51496574be1269dd64ea29ace8c1f4b0	no	3
Warnings:					
Information:					
3	Non Patent Literature	W0537-7010WO_PCTUS2007070701.PDF	619887 8e169ea22bee89ede24145e54f8cb9d4b9188b97	no	13
Warnings:					
Information:					
4	Non Patent Literature	W0537-701810__Npl_-_Challenges.PDF	1447509 8ad6a0ceb4c627ea546375cf842225f5ed1ad305	no	27
Warnings:					
Information:					
5	Information Disclosure Statement (IDS) Form (SB08)	Information_Disclosure_Statement_Fillable_PDF.PDF	615379 ff14f7b2b283fb5712fa07c684b982b96ee371e0	no	14
Warnings:					
Information:					
6	Foreign Reference	WO9207436A1.PDF	889520 7098a34759ce7c01214023cc06d65a819d473cdb	no	25
Warnings:					
Information:					
7	Foreign Reference	WO2012037479A9A9.PDF	4492129 3c262401fd526de8a0379696b7589a5652470f4a	no	101
Warnings:					
Information:					
8	Foreign Reference	WO2002014985A2.PDF	2313986 f14647afc0976ee833d254aacb6a5fe3ae5e87e	no	50

Warnings:					
Information:					
9	Foreign Reference	WO96036934A1.PDF	7289165 007fd711922f2779adb32215e9baf42dc7dedd6b	no	206
Warnings:					
Information:					
10	Foreign Reference	WO92007436A1.PDF	878762 65dd797f450466a3aaa2fc05d64fa60a4dd5585d	no	25
Warnings:					
Information:					
11	Foreign Reference	GB2382006A.PDF	2200771 188a531f7ef9a7ce40f893fc386bcd2e5fc366f	no	53
Warnings:					
Information:					
12	Foreign Reference	EP1081632A1.PDF	822354 18923482579bfb496672c926aa783f3b3e2190d	no	15
Warnings:					
Information:					
13	Foreign Reference	EP986209A2.PDF	1355172 e95cf4820b7a023ea59df994c62595e0a088866f	no	20
Warnings:					
Information:					
14	Fee Worksheet (SB06)	fee-info.pdf	30180 d9235c4774ccc1e016661c1f81d8c2841b2b068c	no	2
Warnings:					
Information:					
Total Files Size (in bytes):				23674159	

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with 37 CFR § 1.6(a)(4).

Dated: March 28, 2014
Electronic Signature for Matthew H. Grady: /Matthew H. Grady/

Docket No.: W0537-700620
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Kenneth P. Weiss

Allowed: February 28, 2014

Application No.: 11/768,729

Confirmation No.: 3536

Filed: June 26, 2007

Art Unit: 2435

For: UNIVERSAL SECURE REGISTRY

Examiner: B. W. Dada

INFORMATION DISCLOSURE STATEMENT (IDS)

Commissioner for Patents

Dear Madam:

Pursuant to 37 C.F.R. § 1.56, 1.97 and 1.98, the attention of the Patent and Trademark Office is hereby directed to the references listed on the attached PTO/SB/08. It is respectfully requested that the information be expressly considered during the prosecution of this application, and that the references be made of record therein and appear among the "References Cited" on any patent to issue therefrom.

This Information Disclosure Statement, pursuant to 37 C.F.R. § 1.114(c), accompanies the Request for Continued Examination (37 C.F.R. § 1.114) submitted herewith.

In accordance with 37 C.F.R. § 1.98(a)(2)(ii), Applicant has not submitted copies of U.S. patents and U.S. patent applications. Applicant submits herewith copies of foreign patents and non-patent literature in accordance with 37 C.F.R. § 1.98(a)(2).

In accordance with 37 C.F.R. § 1.97(g), the filing of this Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material

information as defined in 37 C.F.R. § 1.56(a) exists. In accordance with 37 C.F.R. § 1.97(h), the filing of this Information Disclosure Statement shall not be construed to be an admission that any patent, publication or other information referred to therein is “prior art” for this invention unless specifically designated as such.

It is submitted that the Information Disclosure Statement is in compliance with 37 C.F.R. § 1.98 and the Examiner is respectfully requested to consider the listed references.

The Director is hereby authorized to charge any deficiency in the fees filed, asserted to be filed or which should have been filed herewith (or with any paper hereafter filed in this application by this firm) to our Deposit Account No. 50/2762, under Order No. W0537-700620.

Dated: March 28, 2014

Respectfully submitted,

Electronic signature: /Matthew H. Grady/
Matthew H. Grady

Registration No.: 52,957
LANDO & ANASTASI LLP
Riverfront Office Park
One Main Street
Suite 1100
Cambridge, Massachusetts 02142
(617) 395-7000
Attorney for Applicant



UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

37462 7590 05/23/2014
LANDO & ANASTASI, LLP
ONE MAIN STREET, SUITE 1100
CAMBRIDGE, MA 02142

EXAMINER
GYORFI, THOMAS A
ART UNIT PAPER NUMBER

2435

DATE MAILED: 05/23/2014

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.

TITLE OF INVENTION: UNIVERSAL SECURE REGISTRY

Table with 7 columns: APPLN. TYPE, ENTITY STATUS, ISSUE FEE DUE, PUBLICATION FEE DUE, PREV. PAID ISSUE FEE, TOTAL FEE(S) DUE, DATE DUE

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the ENTITY STATUS shown above. If the ENTITY STATUS is shown as SMALL or MICRO, verify whether entitlement to that entity status still applies.

If the ENTITY STATUS is the same as shown above, pay the TOTAL FEE(S) DUE shown above.

If the ENTITY STATUS is changed from that shown above, on PART B - FEE(S) TRANSMITTAL, complete section number 5 titled "Change in Entity Status (from status indicated above)".

For purposes of this notice, small entity fees are 1/2 the amount of undiscounted fees, and micro entity fees are 1/2 the amount of small entity fees.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PART B - FEE(S) TRANSMITTAL

**Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE
 Commissioner for Patents
 P.O. Box 1450
 Alexandria, Virginia 22313-1450
 or Fax (571)-273-2885**

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

37462 7590 05/23/2014
LANDO & ANASTASI, LLP
 ONE MAIN STREET, SUITE 1100
 CAMBRIDGE, MA 02142

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/768,729	06/26/2007	Kenneth P. Weiss	W0537-700620	3536

TITLE OF INVENTION: UNIVERSAL SECURE REGISTRY

APPLN. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$480	\$0	\$0	\$480	08/25/2014

EXAMINER	ART UNIT	CLASS-SUBCLASS
GYORFI, THOMAS A	2435	713-182000

<p>1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).</p> <p><input type="checkbox"/> Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.</p> <p><input type="checkbox"/> "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. Use of a Customer Number is required.</p>	<p>2. For printing on the patent front page, list</p> <p>(1) The names of up to 3 registered patent attorneys or agents OR, alternatively, _____ 1</p> <p>(2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. _____ 2</p> <p>_____ 3</p>
---	---

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE _____ (B) RESIDENCE: (CITY and STATE OR COUNTRY) _____

Please check the appropriate assignee category or categories (will not be printed on the patent) : Individual Corporation or other private group entity Government

<p>4a. The following fee(s) are submitted:</p> <p><input type="checkbox"/> Issue Fee</p> <p><input type="checkbox"/> Publication Fee (No small entity discount permitted)</p> <p><input type="checkbox"/> Advance Order - # of Copies _____</p>	<p>4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)</p> <p><input type="checkbox"/> A check is enclosed.</p> <p><input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.</p> <p><input type="checkbox"/> The Director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).</p>
---	--

5. Change in Entity Status (from status indicated above)

Applicant certifying micro entity status. See 37 CFR 1.29

Applicant asserting small entity status. See 37 CFR 1.27

Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO.
Values: 11/768,729, 06/26/2007, Kenneth P. Weiss, W0537-700620, 3536

37462 7590 05/23/2014
LANDO & ANASTASI, LLP
ONE MAIN STREET, SUITE 1100
CAMBRIDGE, MA 02142

EXAMINER

GYORFI, THOMAS A

ART UNIT PAPER NUMBER

2435

DATE MAILED: 05/23/2014

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(Applications filed on or after May 29, 2000)

The Office has discontinued providing a Patent Term Adjustment (PTA) calculation with the Notice of Allowance.

Section 1(h)(2) of the AIA Technical Corrections Act amended 35 U.S.C. 154(b)(3)(B)(i) to eliminate the requirement that the Office provide a patent term adjustment determination with the notice of allowance. See Revisions to Patent Term Adjustment, 78 Fed. Reg. 19416, 19417 (Apr. 1, 2013). Therefore, the Office is no longer providing an initial patent term adjustment determination with the notice of allowance. The Office will continue to provide a patent term adjustment determination with the Issue Notification Letter that is mailed to applicant approximately three weeks prior to the issue date of the patent, and will include the patent term adjustment on the patent. Any request for reconsideration of the patent term adjustment determination (or reinstatement of patent term adjustment) should follow the process outlined in 37 CFR 1.705.

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

OMB Clearance and PRA Burden Statement for PTOL-85 Part B

The Paperwork Reduction Act (PRA) of 1995 requires Federal agencies to obtain Office of Management and Budget approval before requesting most types of information from the public. When OMB approves an agency request to collect information from the public, OMB (i) provides a valid OMB Control Number and expiration date for the agency to display on the instrument that will be used to collect the information and (ii) requires the agency to inform the public about the OMB Control Number's legal significance in accordance with 5 CFR 1320.5(b).

The information collected by PTOL-85 Part B is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450. Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Notice of Allowability	Application No. 11/768,729	Applicant(s) WEISS, KENNETH P.	
	Examiner Thomas Gyorfi	Art Unit 2435	AIA (First Inventor to File) Status No

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. This communication is responsive to the RCE filed 3/28/14.
 A declaration(s)/affidavit(s) under 37 CFR 1.130(b) was/were filed on _____.
2. An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.
3. The allowed claim(s) is/are 1,3-5,9-16,19-21,24-30,32-39 and 41-48. As a result of the allowed claim(s), you may be eligible to benefit from the **Patent Prosecution Highway** program at a participating intellectual property office for the corresponding application. For more information, please see http://www.uspto.gov/patents/init_events/pph/index.jsp or send an inquiry to PPHfeedback@uspto.gov.
4. Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

Certified copies:

- a) All b) Some *c) None of the:
1. Certified copies of the priority documents have been received.
 2. Certified copies of the priority documents have been received in Application No. _____.
 3. Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

* Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.


THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
 including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.
Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
6. DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

- | | |
|--|---|
| <ol style="list-style-type: none"> 1. <input type="checkbox"/> Notice of References Cited (PTO-892) 2. <input checked="" type="checkbox"/> Information Disclosure Statements (PTO/SB/08),
Paper No./Mail Date <u>3/28/14</u> 3. <input type="checkbox"/> Examiner's Comment Regarding Requirement for Deposit of Biological Material 4. <input type="checkbox"/> Interview Summary (PTO-413),
Paper No./Mail Date _____. | <ol style="list-style-type: none"> 5. <input type="checkbox"/> Examiner's Amendment/Comment 6. <input type="checkbox"/> Examiner's Statement of Reasons for Allowance 7. <input type="checkbox"/> Other _____. |
|--|---|


/Darren B Schwartz/
Primary Examiner, Art Unit 2435

Issue Classification 	Application/Control No. 11768729	Applicant(s)/Patent Under Reexamination WEISS, KENNETH P.	
	Examiner THOMAS GYORFI	Art Unit 2435	

CPC						
Symbol					Type	Version
G06F		21		6245	I	2013-01-01
Y10S		707		99931	A	2013-01-01
Y10S		707		99933	A	2013-01-01
H04L		63		105	F	2013-01-01
Y10S		707		99939	A	2013-01-01
G06Q		20		382	I	2013-01-01
H04L		2463		102	A	2013-01-01

CPC Combination Sets				
Symbol	Type	Set	Ranking	Version

/THOMAS GYORFI/ Examiner.Art Unit 2435 (Assistant Examiner)	5/17/14 (Date)	Total Claims Allowed: 38	
/DARREN B SCHWARTZ/ Primary Examiner.Art Unit 2435 (Primary Examiner)	05/18/2014 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 1

Issue Classification 	Application/Control No. 11768729	Applicant(s)/Patent Under Reexamination WEISS, KENNETH P.
	Examiner THOMAS GYORFI	Art Unit 2435

<input type="checkbox"/> Claims renumbered in the same order as presented by applicant		<input type="checkbox"/> CPA		<input type="checkbox"/> T.D.		<input type="checkbox"/> R.1.47									
Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1		17	12	33										
	2		18	13	34										
2	3	23	19	14	35										
3	4	24	20	15	36										
4	5	25	21	34	37										
	6		22	35	38										
	7		23	36	39										
	8	26	24		40										
5	9	27	25	16	41										
6	10	29	26	17	42										
7	11	30	27	18	43										
8	12	31	28	19	44										
9	13	32	29	20	45										
10	14	33	30	21	46										
11	15		31	37	47										
22	16	28	32	38	48										

/THOMAS GYORFI/ Examiner.Art Unit 2435 (Assistant Examiner)	5/17/14 (Date)	Total Claims Allowed: 38	
/DARREN B SCHWARTZ/ Primary Examiner.Art Unit 2435 (Primary Examiner)	05/18/2014 (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 1

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		11768729
	Filing Date		2007-06-26
	First Named Inventor	Kenneth P. Weiss	
	Art Unit		2435
	Examiner Name	B. W. Dada	
	Attorney Docket Number		W0537-700620

U.S.PATENTS						Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages,Columns,Lines where Relevant Passages or Relevant Figures Appear
	1	4720860		1988-01-19	Weiss	
	2	4856062		1989-08-08	Weiss	
	3	4885778		1989-12-05	Weiss	
	4	4998279		1991-03-05	Weiss	
	5	5023908		1991-06-11	Weiss	
	6	5058161		1991-10-15	Weiss	
	7	5097505		1992-03-17	Weiss	
	8	5168520		1992-12-01	Weiss	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		11768729
Filing Date		2007-06-26
First Named Inventor	Kenneth P. Weiss	
Art Unit		2435
Examiner Name	B. W. Dada	
Attorney Docket Number		W0537-700620

	9	5237614		1993-08-17	Weiss	
	10	5361062		1994-11-01	Weiss et al.	
	11	5367572		1994-11-22	Weiss	
	12	5398285		1995-03-14	Borgelt et al.	
	13	5479512		1995-12-26	Weiss	
	14	5485519		1996-01-16	Weiss	
	15	5664109		1997-09-02	Johnson et al.	
	16	5813006		1998-09-22	Polnerow et al.	
	17	5870723		1999-02-09	Pare, Jr. et al.	
	18	5915023		1999-06-22	Bernstein	
	19	6073106		2000-06-06	Rozen et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		11768729
Filing Date		2007-06-26
First Named Inventor	Kenneth P. Weiss	
Art Unit		2435
Examiner Name	B. W. Dada	
Attorney Docket Number		W0537-700620

	20	6088450		2000-07-11	Davis et al.	
	21	6130621		2000-10-10	Weiss	
	22	6202055		2001-03-13	Houvener et al.	
	23	6253202		2001-06-26	Gilmour	
	24	6253203		2001-06-26	O'Flaherty et al.	
	25	6260039		2001-07-10	Schneck et al.	
	26	6308203		2001-10-23	Itabashi et al.	
	27	6309342		2001-10-30	Blazey et al.	
	28	6393421		2002-05-21	Paglin	
	29	6516315		2003-02-04	Gupta	
	30	6546005		2003-04-08	Berkley et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	11768729
Filing Date	2007-06-26
First Named Inventor	Kenneth P. Weiss
Art Unit	2435
Examiner Name	B. W. Dada
Attorney Docket Number	W0537-700620

31	6581059		2003-06-17	Barrett et al.	
32	6640211		2003-10-28	Holden	
33	6658400		2003-12-02	Perell et al.	
34	6819219		2004-11-16	Bolle et al.	
35	6845448		2005-01-18	Chaganti et al.	
36	6941271		2005-09-06	Soong	
37	7007298		2006-02-28	Shinzaki et al.	
38	7249112		2007-07-24	Berardi et al.	
39	7278026		2007-10-02	McGowan	
40	7412604		2008-08-12	Doyle	
41	7489781		2009-02-10	Klassen et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	11768729
Filing Date	2007-06-26
First Named Inventor	Kenneth P. Weiss
Art Unit	2435
Examiner Name	B. W. Dada
Attorney Docket Number	W0537-700620

42	7502459		2009-03-10	Moseley	
43	7548981		2009-06-16	Taylor et al.	
44	7552333		2009-06-23	Wheeler et al.	
45	7571139		2009-08-04	Giordano et al.	
46	7657639		2010-02-02	Hinton	
47	7705732		2010-04-27	Bishop et al.	
48	8079079		2011-12-13	Zhang et al.	

If you wish to add additional U.S. Patent citation information please click the Add button.

[Add](#)

U.S.PATENT APPLICATION PUBLICATIONS

[Remove](#)

Examiner Initial*	Cite No	Publication Number	Kind Code ¹	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear
	1	20010032100		2001-10-18	Mahmud et al.	
	2	20010044900		2001-11-22	Uchida	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		11768729
Filing Date		2007-06-26
First Named Inventor	Kenneth P. Weiss	
Art Unit		2435
Examiner Name	B. W. Dada	
Attorney Docket Number		W0537-700620

3	20020046061		2002-04-18	Wright et al.	
4	20020090930		2002-07-11	Fujiwara et al.	
5	20020176610		2002-11-28	Okazaki et al.	
6	20020178364		2002-11-28	Weiss	
7	20030014372		2003-01-16	Wheeler et al.	
8	20030115490		2003-06-19	Russo et al.	
9	20030123713		2003-07-03	Geng	
10	20030129965		2003-07-10	Siegel	
11	20030163710		2003-08-28	Ortiz et al.	
12	20030226041		2003-12-04	Palmer et al.	
13	20040017934		2004-01-29	Kocher	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		11768729
Filing Date		2007-06-26
First Named Inventor	Kenneth P. Weiss	
Art Unit		2435
Examiner Name	B. W. Dada	
Attorney Docket Number		W0537-700620

14	20040034771		2004-02-19	Edgett et al.	
15	20040059923		2004-03-25	ShamRao	
16	20040111625		2004-06-10	Duffy et al.	
17	20040117215		2004-06-17	Marchosky	
18	20040117302		2004-06-17	Weichert et al.	
19	20040133787		2004-07-08	Doughty et al.	
20	20040151351		2004-08-05	Ito	
21	20040188519		2004-09-30	Cassone	
22	20040236699		2004-11-25	Beenau et al.	
23	20050001711		2005-01-06	Doughty et al.	
24	20050039027		2005-02-17	Shapiro	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		11768729
Filing Date		2007-06-26
First Named Inventor	Kenneth P. Weiss	
Art Unit		2435
Examiner Name	B. W. Dada	
Attorney Docket Number		W0537-700620

	25	20050187843		2005-08-25	Lapsley et al.	
	26	20050187873		2005-08-25	Labrou et al.	
	27	20050210270		2005-09-22	Rohatgi et al.	
	28	20050235148		2005-10-20	Scheidt et al.	
	29	20050238208		2005-10-27	Sim	
	30	20060000900		2006-01-05	Fernandes et al.	
	31	20060016884		2006-01-26	Block et al.	
	32	20060104486		2006-05-18	Le Saint et al.	
	33	20060122939		2006-06-08	Cohen et al.	
	34	20060165060		2006-07-27	Dua	
	35	20060206724		2006-09-14	Schaufele et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		11768729
Filing Date		2007-06-26
First Named Inventor	Kenneth P. Weiss	
Art Unit		2435
Examiner Name	B. W. Dada	
Attorney Docket Number		W0537-700620

	36	20060256961		2006-11-16	Brainard et al.	
	37	20070005988		2007-01-04	Zhang et al.	
	38	20070040017		2007-02-22	Kozlay	
	39	20070079136		2007-04-05	Vishik et al.	
	40	20070124597		2007-05-31	Bedingfield	
	41	20070124697		2007-05-31	Dongelmans	
	42	20070140145		2007-06-21	Kumar et al.	
	43	20070186105		2007-08-09	Bailey et al.	
	44	20070186115		2007-08-09	GAO et al.	
	45	20070198436		2007-08-23	Weiss	
	46	20070245152		2007-10-18	Pizano et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number		11768729
Filing Date		2007-06-26
First Named Inventor	Kenneth P. Weiss	
Art Unit		2435
Examiner Name	B. W. Dada	
Attorney Docket Number		W0537-700620

47	20080005576		2008-01-03	Weiss	
48	20080021997		2008-01-24	HINTON	
49	20080040274		2008-02-14	UZO	
50	20080127311		2008-05-29	Yasaki et al.	
51	20080212848		2008-09-04	Doyle	
52	20080275819		2008-11-06	Rifai	
53	20090083544		2009-03-26	Scholnick et al.	
54	20090144814		2009-06-04	Sacco	
55	20090175507		2009-07-09	Schaffner	
56	20090203355		2009-08-13	Clark	
57	20100046443		2010-02-25	Jia et al.	

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	11768729
Filing Date	2007-06-26
First Named Inventor	Kenneth P. Weiss
Art Unit	2435
Examiner Name	B. W. Dada
Attorney Docket Number	W0537-700620

58	20120130904		2012-05-24	Weiss	
59	20120240195		2012-09-20	Weiss	

If you wish to add additional U.S. Published Application citation information please click the Add button. [Add](#)

FOREIGN PATENT DOCUMENTS

[Remove](#)

Examiner Initial*	Cite No	Foreign Document Number ³	Country Code ² i	Kind Code ⁴	Publication Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	T ⁵
	1	0986209	EP	A2	2000-03-15	Mitsubishi Electric Corp		<input type="checkbox"/>
	2	1081632	EP	A1	2001-03-07	Keyware, Technologies		<input type="checkbox"/>
	3	2382006	GB	A	2003-05-14	Ibm		<input type="checkbox"/>
	4	0214985	WO	A2	2002-02-21	Kern, Daniel		<input type="checkbox"/>
	5	1992007436	WO	A1	1992-04-30	Security Dynamics Techn		<input type="checkbox"/>
	6	1996036934	WO	A1	1996-11-21	Smart Touch L L C		<input type="checkbox"/>
	7	2012037479	WO	A1	2012-03-22	Universal Secure Registry, Llc		<input type="checkbox"/>

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		11768729	
	Filing Date		2007-06-26	
	First Named Inventor	Kenneth P. Weiss		
	Art Unit		2435	
	Examiner Name	B. W. Dada		
	Attorney Docket Number		W0537-700620	

	8	9207436	WO	A1	1992-04-30	Security Dynamics Technologies, Inc	<input type="checkbox"/>
--	---	---------	----	----	------------	-------------------------------------	--------------------------

If you wish to add additional Foreign Patent Document citation information please click the Add button **Add**

NON-PATENT LITERATURE DOCUMENTS

Remove

Examiner Initials*	Cite No	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc), date, pages(s), volume-issue number(s), publisher, city and/or country where published.	T ⁵
	1	"Information Security: Challenges in Using Biometrics" 9 September 2003. All pages. < http://www.gao.gov/new.items/d031137t.pdf >	<input type="checkbox"/>
	2	International Search Report from PCT/US2007/070701 mailed March 11, 2008	<input type="checkbox"/>

If you wish to add additional non-patent literature document citation information please click the Add button **Add**

EXAMINER SIGNATURE

Examiner Signature	/Thomas Gyorfi/	Date Considered	05/17/2014
--------------------	-----------------	-----------------	------------

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through a citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

¹ See Kind Codes of USPTO Patent Documents at www.USPTO.GOV or MPEP 901.04. ² Enter office that issued the document, by the two-letter code (WIPO Standard ST.3). ³ For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. ⁴ Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. ⁵ Applicant is to place a check mark here if English language translation is attached.

**INFORMATION DISCLOSURE
STATEMENT BY APPLICANT**
(Not for submission under 37 CFR 1.99)

Application Number	11768729		
Filing Date	2007-06-26		
First Named Inventor	Kenneth P. Weiss		
Art Unit	2435		
Examiner Name	B. W. Dada		
Attorney Docket Number	W0537-700620		

CERTIFICATION STATEMENT

Please see 37 CFR 1.97 and 1.98 to make the appropriate selection(s):

That each item of information contained in the information disclosure statement was first cited in any communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(1).

OR

That no item of information contained in the information disclosure statement was cited in a communication from a foreign patent office in a counterpart foreign application, and, to the knowledge of the person signing the certification after making reasonable inquiry, no item of information contained in the information disclosure statement was known to any individual designated in 37 CFR 1.56(c) more than three months prior to the filing of the information disclosure statement. See 37 CFR 1.97(e)(2).

- See attached certification statement.
- The fee set forth in 37 CFR 1.17 (p) has been submitted herewith.
- A certification statement is not submitted herewith.

SIGNATURE

A signature of the applicant or representative is required in accordance with CFR 1.33, 10.18. Please see CFR 1.4(d) for the form of the signature.

Signature	/Matthew H. Grady/	Date (YYYY-MM-DD)	2014-03-28
Name/Print	Matthew H. Grady	Registration Number	52957

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 1 hour to complete, including gathering, preparing and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. **DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

Privacy Act Statement

The Privacy Act of 1974 (P.L. 93-579) requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C. 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether the Freedom of Information Act requires disclosure of these records.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (i.e., GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspections or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /TG/

EAST Search History

EAST Search History (Prior Art)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	283	"5657388".uref.	US-PGPUB; USPAT	OR	OFF	2014/05/17 16:00
L2	27	L1 and @ad<"20010316"	US-PGPUB; USPAT	OR	OFF	2014/05/17 16:00
L3	11	L2 and restrict\$3	US-PGPUB; USPAT	OR	OFF	2014/05/17 16:00
L4	1533	713/169.ccls.	US-PGPUB; USPAT	OR	OFF	2014/05/17 16:00
L5	3316	713/182.ccls.	US-PGPUB; USPAT	OR	OFF	2014/05/17 16:00
L6	1007	713/184.ccls.	US-PGPUB; USPAT	OR	OFF	2014/05/17 16:00
L7	769	(L3 L4 L5 L6) and @ad<"20010316"	US-PGPUB; USPAT	OR	OFF	2014/05/17 16:00
L8	16	L7 and (provider same (token timecode (time near2 code)))	US-PGPUB; USPAT	OR	OFF	2014/05/17 16:01
L9	0	L7 and (universal adj secure adj registry).as.	US-PGPUB; USPAT	OR	OFF	2014/05/17 16:01
L10	2	(("20120130904") or ("20120240195")).PN.	US-PGPUB; USPAT	OR	OFF	2014/05/17 16:02
L11	94	US-4720860-\$.DID. OR US-4856062-\$.DID. OR US-4885778-\$.DID. OR US-4998279-\$.DID. OR US-5023908-\$.DID. OR US-5058161-\$.DID. OR US-5097505-\$.DID. OR US-5168520-\$.DID. OR US-5237614-\$.DID. OR US-5361062-\$.DID. OR US-5367572-\$.DID. OR US-5398285-\$.DID. OR US-5479512-\$.DID. OR US-5485519-\$.DID. OR US-5664109-\$.DID. OR US-5813006-\$.DID. OR US-5870723-\$.DID. OR US-5915023-\$.DID. OR US-6073106-\$.DID. OR US-6088450-\$.DID. OR US-6130621-\$.DID. OR US-6202055-\$.DID. OR US-6253202-\$.DID. OR US-6253203-\$.DID. OR US-6260039-\$.DID. OR US-6308203-\$.DID. OR US-6309342-\$.DID. OR US-6393421-\$.DID. OR US-6516315-\$.DID. OR US-6546005-\$.DID. OR US-6581059-\$.DID. OR US-6640211-\$.DID. OR US-6658400-\$.DID. OR US-	US-PGPUB; USPAT; USOCR	OR	OFF	2014/05/17 16:04

		6819219-\$.DID. OR US-6845448-\$.DID. OR US-6941271-\$.DID. OR US-7007298-\$.DID. OR US-7249112-\$.DID. OR US-7278026-\$.DID. OR US-7412604-\$.DID. OR US-7489781-\$.DID. OR US-7502459-\$.DID. OR US-7548981-\$.DID. OR US-7552333-\$.DID. OR US-7571139-\$.DID. OR US-7657639-\$.DID. OR US-7705732-\$.DID. OR US-8079079-\$.DID. OR US-20010032100-\$.DID. OR US-20010044900-\$.DID. OR US-20020046061-\$.DID. OR US-20020090930-\$.DID. OR US-20020176610-\$.DID. OR US-20020178364-\$.DID. OR US-20030014372-\$.DID. OR US-20030115490-\$.DID. OR US-20030123713-\$.DID. OR US-20030129965-\$.DID. OR US-20030163710-\$.DID. OR US-20030226041-\$.DID. OR US-20040017934-\$.DID. OR US-20040034771-\$.DID. OR US-20040059923-\$.DID. OR US-20040111625-\$.DID. OR US-20040117215-\$.DID. OR US-20040117302-\$.DID. OR US-20040133787-\$.DID. OR US-20040151351-\$.DID. OR US-20040188519-\$.DID. OR US-20040236699-\$.DID. OR US-20050001711-\$.DID. OR US-20050039027-\$.DID. OR US-20050187843-\$.DID. OR US-20050187873-\$.DID. OR US-20050210270-\$.DID. OR US-20050235148-\$.DID. OR US-20050238208-\$.DID. OR US-20060000900-\$.DID. OR US-20060016884-\$.DID. OR US-20060104486-\$.DID. OR US-20060122939-\$.DID. OR US-20060165060-\$.DID. OR US-20060206724-\$.DID. OR US-20060256961-\$.DID. OR US-20070005988-\$.DID. OR US-20070040017-\$.DID. OR US-20070079136-\$.DID. OR US-20070124597-\$.DID. OR US-20070124697-\$.DID. OR US-20070140145-\$.DID. OR US-20070186105-\$.DID. OR US-20070186115-\$.DID. OR US-20070198436-\$.DID. OR US-20070245152-\$.DID.				
L12	11	US-20080005576-\$.DID. OR US-20080021997-\$.DID. OR US-20080040274-\$.DID. OR US-20080127311-\$.DID. OR US-20080212848-\$.DID. OR US-20080275819-\$.DID. OR US-20090083544-\$.DID. OR US-20090144814-\$.DID. OR US-20090175507-\$.DID. OR US-20090203355-\$.DID. OR US-20100046443-\$.DID.	US-PGPUB; USPAT; USOCR	OR	OFF	2014/05/17 16:06
S1	3	(("6018724") or ("7571139") or ("5657388")).PN.	US-PGPUB; USPAT	OR	OFF	2013/08/22 17:35
S2	8	US-6498861-\$.DID. OR US-7237117-\$.DID. OR US-5457747-\$.DID. OR US-6950521-\$.DID. OR US-8001055-\$.DID. OR US-7809651-\$.DID. OR US-7805372-\$.DID. OR US-8234220-\$.DID.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/08/23 15:40
S3	9	US-7766223-\$.DID. OR US-20030229637-\$.DID. OR US-20030046540-\$.DID. OR US-20020184538-\$.DID. OR US-20030028481-\$.DID. OR US-20030084332-\$.DID. OR US-20030085808-\$.DID. OR US-20050113070-\$.DID. OR US-20050238147-\$.DID.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/08/23 15:41

S4	6	US-20070256120-\$.DID. OR US-20090292641-\$.DID. OR US-20100000455-\$.DID. OR US-20110258120-\$.DID. OR US-20130024374-\$.DID. OR US-20120037479-\$.DID.	US-PGPUB; USPAT; USOCR	OR	OFF	2013/08/23 15:42
S5	254	"5657388".uref.	US-PGPUB; USPAT	OR	OFF	2013/09/25 16:30
S6	27	S5 and @ad<"20010316"	US-PGPUB; USPAT	OR	OFF	2013/09/25 16:31
S7	11	S6 and restrict\$3	US-PGPUB; USPAT	OR	OFF	2013/09/25 16:37
S8	1390	713/169.ccls.	US-PGPUB; USPAT	OR	OFF	2013/09/25 16:56
S9	3037	713/182.ccls.	US-PGPUB; USPAT	OR	OFF	2013/09/25 16:57
S10	917	713/184.ccls.	US-PGPUB; USPAT	OR	OFF	2013/09/25 16:57
S11	0	707/9.ccls.	US-PGPUB; USPAT	OR	OFF	2013/09/25 16:57
S12	2927	707/999.009.ccls.	US-PGPUB; USPAT	OR	OFF	2013/09/25 16:58
S13	1634	(S8 S9 S10 S12) and @ad<"20010316"	US-PGPUB; USPAT	OR	OFF	2013/09/25 16:58
S14	318	S13 and (token timecode (time near2 code))	US-PGPUB; USPAT	OR	OFF	2013/09/25 16:59
S15	152	S14 and restrict\$3	US-PGPUB; USPAT	OR	OFF	2013/09/25 16:59
S16	1	("7571139").PN.	US-PGPUB; USPAT	OR	OFF	2014/01/24 10:15
S17	1468	713/169.ccls.	US-PGPUB; USPAT	OR	OFF	2014/02/14 16:36
S18	3218	713/182.ccls.	US-PGPUB; USPAT	OR	OFF	2014/02/14 16:36
S19	979	713/184.ccls.	US-PGPUB; USPAT	OR	OFF	2014/02/14 16:36
S20	2933	707/999.009.ccls.	US-PGPUB; USPAT	OR	OFF	2014/02/14 16:36
S21	400	secure near2 registry	US-PGPUB; USPAT	OR	OFF	2014/02/14 16:48
S22	1	S21 and (provider same (token timecode	US-	OR	OFF	2014/02/14


		(time near2 code)))	PGPUB; USPAT			16:48
S23	0	S21 and (provider same securid)	US- PGPUB; USPAT	OR	OFF	2014/02/14 16:49
S24	13	(S17 S18 S19 S20) and secure near2 registry	US- PGPUB; USPAT	OR	OFF	2014/02/14 16:49
S25	1	("20080005576").PN.	US- PGPUB; USPAT	OR	OFF	2014/02/14 17:29
S31	8315	weiss.in.	US- PGPUB; USPAT	OR	OFF	2014/02/21 19:00
S32	103	S31 and (ken.in. kenneth.in.)	US- PGPUB; USPAT	OR	OFF	2014/02/21 19:01
S33	7	(universal adj secure adj registry).as.	US- PGPUB; USPAT	OR	OFF	2014/02/21 19:01
S34	30	S32 and @ad<"20010316"	US- PGPUB; USPAT	OR	OFF	2014/02/21 19:02

EAST Search History (Interference)

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
S26	231	secure near2 registry	US-PGPUB; UPAD	OR	OFF	2014/02/14 17:33
S27	91107	(token timecode (time near2 code) securid)	US-PGPUB; UPAD	OR	OFF	2014/02/14 17:34
S28	104	S27 and S26	US-PGPUB; UPAD	OR	OFF	2014/02/14 17:34
S29	4980	S27 same provider	US-PGPUB; UPAD	OR	OFF	2014/02/14 17:34
S30	1	S29 and S26	US-PGPUB; UPAD	OR	OFF	2014/02/14 17:34

5/17/2014 4:06:33 PM

C:\Users\tyorfi\Documents\EAST\Workspaces\11768729.wsp

Search Notes 	Application/Control No. 11768729	Applicant(s)/Patent Under Reexamination WEISS, KENNETH P.
	Examiner BEEMNET W DADA	Art Unit 2435

CPC- SEARCHED		
Symbol	Date	Examiner

CPC COMBINATION SETS - SEARCHED		
Symbol	Date	Examiner

US CLASSIFICATION SEARCHED			
Class	Subclass	Date	Examiner
713	169, 182, 184	12/10/2012	BD
707	9	12/10/2012	BD
713	169, 182, 184	9/25/13	TAG
707	9	9/25/13	TAG
713	169, 182, 184	2/14/14	TAG
707	999.001	2/14/14	TAG
713	169, 182, 184	5/17/14	TAG
707	999.001	5/17/14	TAG


SEARCH NOTES		
Search Notes	Date	Examiner
East search	12/10/2012	BD
NPL search	12/10/2012	BD
Inventor name search	12/10/2012	BD
EAST search (updated)	9/25/13	TAG
Discussed allowability with SPE J. Hirl (AU2435)	2/10/14	TAG
EAST search (updated)	2/14/14	TAG
NPL search (Google)	2/14/14	TAG
Reviewed by Primary Examiner D. Schwartz (AU 2435)	2/14/14	TAG
EAST search (updated)	5/17/14	TAG

--	--

INTERFERENCE SEARCH

US Class/ CPC Symbol	US Subclass / CPC Group	Date	Examiner
713	182	2/14/14	TAG

--	--

Index of Claims 	Application/Control No. 11768729	Applicant(s)/Patent Under Reexamination WEISS, KENNETH P.
	Examiner THOMAS GYORFI	Art Unit 2435

✓	Rejected
=	Allowed


-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

Claims renumbered in the same order as presented by applicant
 CPA
 T.D.
 R.1.47

CLAIM		DATE							
Final	Original	07/16/2009	09/25/2013	02/14/2014	05/17/2014				
1	1	✓	✓	=	=				
	2	✓	-	-	-				
2	3	✓	✓	=	=				
3	4	✓	✓	=	=				
4	5	✓	✓	=	=				
	6	✓	-	-	-				
	7	✓	-	-	-				
	8	✓	-	-	-				
5	9	✓	✓	=	=				
6	10	✓	✓	=	=				
7	11	✓	✓	=	=				
8	12	✓	✓	=	=				
9	13	✓	✓	=	=				
10	14	✓	✓	=	=				
11	15	✓	✓	=	=				
22	16	✓	✓	=	=				
	17	✓	-	-	-				
	18	✓	-	-	-				
23	19	✓	✓	=	=				
24	20	✓	✓	=	=				
25	21	✓	✓	=	=				
	22	✓	-	-	-				
	23	✓	-	-	-				
26	24	✓	✓	=	=				
27	25	✓	✓	=	=				
29	26	✓	✓	=	=				
30	27	✓	✓	=	=				
31	28	✓	✓	=	=				
32	29	✓	✓	=	=				
33	30	✓	✓	=	=				
	31		-	-	-				
28	32		✓	=	=				
12	33		✓	=	=				
13	34		✓	=	=				
14	35		✓	=	=				
15	36		✓	=	=				

<i>Index of Claims</i> 	Application/Control No. 11768729	Applicant(s)/Patent Under Reexamination WEISS, KENNETH P.
	Examiner THOMAS GYORFI	Art Unit 2435

✓	Rejected
=	Allowed

-	Cancelled
÷	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

Claims renumbered in the same order as presented by applicant
 CPA
 T.D.
 R.1.47

CLAIM		DATE							
Final	Original	07/16/2009	09/25/2013	02/14/2014	05/17/2014				
34	37		✓	=	=				
35	38		✓	=	=				
36	39		✓	=	=				
	40		-	-	-				
16	41		✓	=	=				
17	42		✓	=	=				
18	43		✓	=	=				
19	44		✓	=	=				
20	45		✓	=	=				
21	46		✓	=	=				
37	47		✓	=	=				
38	48		✓	=	=				

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: **Mail** **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax **(571)-273-2885**

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

~~Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.~~

37462 7596 05/23/2014
LANDO & ANASTASI, LLP
ONE MAIN STREET, SUITE 1100
CAMBRIDGE, MA 02142

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

	(Depositor's name)
	(Signature)
	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/768,729	06/26/2007	Kenneth P. Weiss	W0537-700620	3536

TITLE OF INVENTION: UNIVERSAL SECURE REGISTRY

APPL. TYPE	ENTITY STATUS	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	SMALL	\$480	\$0	\$0	\$480	08/25/2014

EXAMINER	ART UNIT	CLASS-SUBCLASS
GYOREI, THOMAS A	2435	713-182000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363). <input type="checkbox"/> Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached. <input checked="" type="checkbox"/> "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. Use of a Customer Number is required.	2. For printing on the patent front page, list (1) The names of up to 3 registered patent attorneys or agents OR, alternatively, (2) The name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.	1. Lando & Anastasi, LLP 2. _____ 3. _____
---	---	---

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: **UNIVERSAL SECURE REGISTRY, LLC**

(B) RESIDENCE: (CITY and STATE OR COUNTRY) **Newton, MA**

Please check the appropriate assignee category or categories (will not be printed on the patent): Individual Corporation or other private group entity Government

4a. The following fee(s) are submitted: <input checked="" type="checkbox"/> Issue Fee <input type="checkbox"/> Publication Fee (No small entity discount permitted) <input type="checkbox"/> Advance Order - # of Copies _____	4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above) <input type="checkbox"/> A check is enclosed. <input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached. <input checked="" type="checkbox"/> The Director is hereby authorized to charge the required fee(s), any deficiency, or credits any overpayment, to Deposit Account Number 502762 (enclose an extra copy of this form).
---	---

5. Change in Entity Status (from status indicated above)

Applicant certifying micro entity status. See 37 CFR 1.29

Applicant asserting small entity status. See 37 CFR 1.27

Applicant changing to regular undiscounted fee status.

NOTE: Absent a valid certification of Micro Entity Status (see forms PTO/SB/15A and 15B), issue fee payment in the micro entity amount will not be accepted at the risk of application abandonment.

NOTE: If the application was previously under micro entity status, checking this box will be taken to be a notification of loss of entitlement to micro entity status.

NOTE: Checking this box will be taken to be a notification of loss of entitlement to small or micro entity status, as applicable.

NOTE: This form must be signed in accordance with 37 CFR 1.31 and 1.33. See 37 CFR 1.4 for signature requirements and certifications.

Authorized Signature / Matthew H. Grady / Date August 22, 2014

Typed or printed name Matthew H. Grady Registration No. 52,957

Electronic Patent Application Fee Transmittal

Application Number:	11768729
Filing Date:	26-Jun-2007
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Filer:	Matthew H. Grady
Attorney Docket Number:	W0537-700620

Filed as Small Entity

Utility under 35 USC 111(a) Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Utility Appl Issue Fee	2501	1	480	480

Extension-of-Time:

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Miscellaneous:				
Total in USD (\$)				480

Electronic Acknowledgement Receipt

EFS ID:	19937152
Application Number:	11768729
International Application Number:	
Confirmation Number:	3536
Title of Invention:	UNIVERSAL SECURE REGISTRY
First Named Inventor/Applicant Name:	Kenneth P. Weiss
Customer Number:	37462
Filer:	Matthew H. Grady
Filer Authorized By:	
Attorney Docket Number:	W0537-700620
Receipt Date:	22-AUG-2014
Filing Date:	26-JUN-2007
Time Stamp:	11:44:17
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes
Payment Type	Deposit Account
Payment was successfully received in RAM	\$480
RAM confirmation Number	8448
Deposit Account	502762
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

Charge any Additional Fees required under 37 C.F.R. Section 1.16 (National application filing, search, and examination fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.17 (Patent application and reexamination processing fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.19 (Document supply fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.20 (Post Issuance fees)

Charge any Additional Fees required under 37 C.F.R. Section 1.21 (Miscellaneous fees and charges)

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		Amendment_After_Allowance_Under_37_CFR_1312.pdf	55622 c950078768142d87d00367f7b61015d49f1839e4	yes	10
Multipart Description/PDF files in .zip description					
	Document Description		Start		End
	Amendment after Notice of Allowance (Rule 312)		1		1
	Claims		2		9
	Applicant Arguments/Remarks Made in an Amendment		10		10
Warnings:					
Information:					
2	Issue Fee Payment (PTO-85B)	IssueFeeTransmittal.pdf	184743 1324037ab9ee775e8050e1b016a79933db30411e	no	1
Warnings:					
Information:					
3	Fee Worksheet (SB06)	fee-info.pdf	30198 3d55a836a50d48c9af0fbcc07d3fd4de580dd734	no	2
Warnings:					
Information:					
Total Files Size (in bytes):			270563		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

I hereby certify that this paper (along with any paper referred to as being attached or enclosed) is being transmitted via the Office electronic filing system in accordance with 37 CFR § 1.6(a)(4).

Dated: August 22, 2014
Electronic Signature for Matthew H. Grady: /Matthew H. Grady/

Docket No.: W0537-700620

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Kenneth P. Weiss

Allowed: February 28, 2014

Application No.: 11/768,729

Confirmation No.: 3536

Filed: June 26, 2007

Art Unit: 2435

For: UNIVERSAL SECURE REGISTRY

Examiner: T. A. Gyorfi

AMENDMENT AFTER ALLOWANCE UNDER 37 C.F.R. 1.312

MS Issue Fee
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Madam:

INTRODUCTORY COMMENTS

In response to the Notice of Allowance mailed May 23, 2014, and prior to payment of the issue fee, Applicant respectfully requests consideration and entry of the following amendments to the above-identified application.

Amendments to the Claims are reflected in the listing of claims which begins on page 2 of this paper.

Remarks/Arguments begin on page 10 of this paper.

AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application.

Listing of Claims:

1. (Currently Amended) A secure registry system for providing information to a provider to enable transactions between the provider and entities with secure data stored in the secure registry system, the secure registry system comprising:

a database including secure data for each entity, wherein each entity is associated with a time-varying multicharacter code for each entity having secure data in the secure registry system, respectively, each time-varying multicharacter code representing an identity of one of the respective entities; and

a processor configured to receive a transaction request including at least the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed and an indication of the provider requesting the transaction, to map the time-varying multicharacter code to the identity of the entity-using the time-varying multicharacter code, to execute a restriction mechanism to determine compliance with any access restrictions for the provider to secure data of the entity for completing the transaction based at least in part on the indication of the ~~first party~~ provider and the time-varying multicharacter code of the transaction request, and to allow or not allow access to the secure data associated with the entity including information required to enable the transaction based on the determined compliance with any access restrictions for the provider, the information including account identifying information, wherein the account identifying information is not provided to the provider and the account identifying information is provided to a third party to enable or deny the transaction with the provider without providing the account identifying information to the provider.

2. (Canceled)

3. (Previously Presented) The system of claim 1, wherein the time-varying multicharacter code is provided to the system via a secure electronic transmission device.

4. (Previously Presented) The system of claim 1, wherein the time-varying multicharacter code is encrypted and transmitted to the system, and
wherein the system is configured to decrypt the time-varying multicharacter code with a public key of the entity.
5. (Previously Presented) The system as claimed in claim 1, wherein the transaction includes a service provided by the provider,
wherein said provider's service includes delivery,
wherein the information is an address to which an item is to be delivered to the entity,
wherein the system receives the time-varying multicharacter code, and
wherein the system uses the time-varying multicharacter code to obtain the appropriate address for delivery of the item by the third party.
6. – 8. (Canceled)
9. (Previously Presented) The system as claimed in claim 1, wherein the account identifying information includes credit card account information regarding the entity, and wherein the processor is configured to provide the credit card account information based upon the multicharacter code of the entity to enable the transaction.
10. (Previously Presented) The system as claimed in claim 9, wherein the system is configured to receive an approval of the credit card transaction.
11. (Previously Presented) The system as claimed in claim 1, wherein the account identifying information includes bank card account information regarding the entity, and wherein the processor is configured to provide the bank card account information to enable the transaction based upon the multicharacter code of the entity.
12. (Previously Presented) The system as claimed in claim 11, wherein the system is configured to provide an approval of the bank card transaction.

13. (Previously Presented) The system as claimed in claim 1, wherein the information includes personal identification information regarding the entity.
14. (Previously Presented) The system as claimed in claim 13, wherein the personal identification information comprises a photograph of the entity, and wherein the photograph is provided to the provider.
15. (Previously Presented) The system as claimed in claim 1, wherein the account identifying information identifies email address information regarding the entity.
16. (Previously Presented) A method for providing information to a provider to enable transactions between the provider and entities who have secure data stored in a secure registry in which each entity is identified by a time-varying multicharacter code, the method comprising:
- receiving a transaction request including at least the time-varying multicharacter code for an entity on whose behalf a transaction is to take place and an indication of the provider requesting the transaction;
 - mapping the time-varying multicharacter code to an identity of the entity using the time-varying multicharacter code;
 - determining compliance with any access restrictions for the provider to secure data of the entity for completing the transaction based at least in part on the indication of the provider and the time-varying multicharacter code of the transaction request;
 - accessing information of the entity required to perform the transaction based on the determined compliance with any access restrictions for the provider, the information including account identifying information;
 - providing the account identifying information to a third party without providing the account identifying information to the provider to enable or deny the transaction; and
 - enabling or denying the provider to perform the transaction without the provider's knowledge of the account identifying information.

17. – 18. (Canceled)

19. (Previously Presented) The method of claim 16, wherein the act of receiving the time-varying multicharacter code comprises receiving the time-varying multicharacter code transmitted via a secure electronic transmission device.

20. (Previously Presented) The method of claim 16, wherein the act of receiving the time-varying multicharacter code comprises receiving an encrypted multicharacter code, and wherein the method further comprises decrypting the encrypted multicharacter code.

21. (Previously Presented) The method as claimed in claim 16, wherein the transaction includes a service provided by the provider,
wherein the service includes delivery,
wherein the account identifying information is associated with an address to which an item is to be delivered for the entity, and
wherein the third party receives the address for delivery of an item provided by the provider.

22. – 23. (Canceled)

24. (Previously Presented) The method as claimed in claim 16, wherein the account identifying information includes a credit card number, and wherein the act of using the account identifying information comprises using the credit card number to enable the transaction.

25. (Previously Presented) The method as claimed in claim 24, wherein the act of using the account identifying information comprises receiving a validation or denial of the transaction without providing the credit card number of the entity to the provider.

26. (Previously Presented) The method as claimed in claim 16, wherein the act of using the account identifying information comprises using bank card information about the entity to enable a transaction.

27. (Previously Presented) The method as claimed in claim 26, wherein the act of using the information comprises receiving a validation or denial of the bank card transaction without providing a bank card number of the entity to the provider.
28. (Previously Presented) The method as claimed in claim 16, wherein the act of mapping the time-varying multicharacter code to information required by the provider comprises mapping the time-varying multicharacter code to personal identification information about the entity.
29. (Previously Presented) The method as claimed in claim 28, wherein the personal identification information comprises a photograph of the entity, and
wherein the method further comprises an act of providing the photograph to the provider.
30. (Previously Presented) The method as claimed in claim 16, wherein the account identifying information identifies email address information about the entity.
31. (Canceled)
32. (Previously Presented) The method as claimed in claim 24, further comprising an act of transmitting to the provider one of an approval or a denial of the credit card transaction.
33. (Previously Presented) The system of claim 1, wherein the database is further configured to associate biometric information with each entity having secure data in the secure registry, respectively.
34. (Previously Presented) The system of claim 33, wherein the processor is further configured to map the time-varying multicharacter code to biometric information associated with the entity on whose behalf the transaction is to be performed and to provide the biometric information to the provider.
35. (Previously Presented) The system of claim 34, wherein the biometric information includes an image of the entity on whose behalf the transaction is to be performed.

36. (Previously Presented) The system of claim 34, wherein the time-varying multicharacter code is generated by a device associated with the entity on whose behalf the transaction is to be performed.

37. (Previously Presented) The method as claimed in claim 16, further comprising an act of associating biometric information with each entity having secure data in the secure registry, respectively.

38. (Previously Presented) The method of claim 37, further comprising acts of:
mapping the time-varying multicharacter code to biometric information associated with the entity on whose behalf the transaction is to be performed; and
providing the biometric information to the provider.

39. (Previously Presented) The method of claim 38, wherein the biometric information includes an image of the entity on whose behalf the transaction is to be performed.

40. (Canceled)

41. (Previously Presented) The system of claim 1, wherein the account identifying information includes an account number.

42. (Previously Presented) The system of claim 41, wherein the account identifying information includes credit card account information and the account number includes a credit card number.

43. (Previously Presented) The system of claim 41, wherein the third party includes a financial service provider and the account number includes at least one of a debit card number and a credit card number.

44. (Previously Presented) The system of claim 43, wherein the provider includes a merchant, and the service includes a sale of at least one of goods and services.

45. (Previously Presented) The system of claim 44, wherein the processor is further configured to receive, from the provider, a merchant ID, and a purchase amount.
46. (Previously Presented) The system of claim 1, wherein the identity of the entity is unknown until the time-varying code is mapped to the identity by the processor.
47. (Previously Presented) A secure registry system for providing information to a provider to enable transactions between the provider and entities with secure data stored in the secure registry system, the secure registry system comprising:
- a database including secure data for each entity, wherein each entity is associated with a time-varying multicharacter code for each entity having secure data in the secure registry system, respectively, each time-varying multicharacter code representing an identity of one of the respective entities, wherein the database is configured to permit or deny access to information on the respective entity using the time-varying multicharacter code; and
 - a processor configured to receive the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed, configured to map the time-varying multicharacter code to the identity of the entity to identify the entity, configured to execute a restriction mechanism to determine compliance with any access restrictions for the provider to at least one portion of secure data for completing the transaction and to store an appropriate code with each such portion of secure data, configured to obtain from the database the secure data associated with the entity including information required to enable the transaction, the information including account identifying information, and configured to provide the account identifying information to a third party to enable or deny the transaction without providing the account identifying information to the provider.
48. (Previously Presented) A secure registry system for providing information to a provider to enable transactions between the provider and entities with secure data stored in the secure registry system, the secure registry system comprising:
- a database including secure data for each entity, wherein each entity is associated with a time-varying multicharacter code for each entity having secure data in the secure registry system, respectively, each time-varying multicharacter code representing an identity of one of the respective entities; and

a processor configured to receive the time-varying multicharacter code for the entity on whose behalf a transaction is to be performed, configured to map the time-varying multicharacter code to the identity of the entity without requiring further information to identify the entity, configured to access from the database secure data associated with the entity including information required to enable the transaction, the information including account identifying information, and configured to provide the account identifying information to a third party to enable or deny the transaction without providing the account identifying information to the provider, and wherein enabling or denying the transaction without providing account identifying information to the provider includes limiting transaction information provided by the secure registry system to the provider to transaction approval information.

REMARKS

Claims 1, 3-5, 9-16, 19-21, 24-30, 32-39, and 41-48 were previously pending in this application. Claim 1 has been amended. As a result claims 1, 3-5, 9-16, 19-21, 24-30, 32-39, and 41-48 are pending for examination with claims 1, 16, 47 and 48 being independent claims.

Applicant respectfully requests amendment to Claim 1 to change the phrase “the first party” to “the provider” in one instance to correct antecedent basis issue in claim 1. The change was inadvertently omitted in the Supplemental Amendment filed on January 1, 2014 amending all other instances of “first party” to “provider” in the pending claims. The change to “provider” was discussed with Examiner Gyorfı prior to the supplemental amendment submission and is being requested to make claim 1 consistent with the discussion and the reasons for allowance. Claim 1, as amended, remains allowable for the same reasons identified in the notice of allowance and needs no further search. No new matter has been added as a result of this amendment.

CONCLUSION

Applicant respectfully requests entry of this amendment and issuance of the application. If the Examiner believes this amendment is ineligible for entry under 37 C.F.R. §1.312, the Examiner is requested to call the Applicant’s attorney at the telephone number listed below. If this response is not considered timely filed and if a request for an extension of time is otherwise absent, Applicant hereby requests any necessary extension of time. If there is a fee occasioned by this response, including an extension fee that is not covered by an accompanying payment, please charge any deficiency to Deposit Account No. 50/2762 (Ref. W0537-700620).

Dated: August 22, 2014

Respectfully submitted,

Electronic signature: /Matthew H. Grady/

Matthew H. Grady

Registration No.: 52,957

Marcus E. Browne

Registration No.: 71,897

LANDO & ANASTASI LLP

Riverfront Office Park

One Main Street

Suite 1100

Cambridge, Massachusetts 02142

(617) 395-7000

Attorney for Applicant



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

Table with 5 columns: APPLICATION NO., FILING DATE, FIRST NAMED INVENTOR, ATTORNEY DOCKET NO., CONFIRMATION NO. Includes application details for Kenneth P. Weiss and examiner GYORFI, THOMAS A.

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

docketing@LALaw.com
gengelso@LALaw.com

Response to Rule 312 Communication	Application No. 11/768,729	Applicant(s) WEISS, KENNETH P.
	Examiner Thomas Gyorfi	Art Unit 2435

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

1. The amendment filed on 22 August 2014 under 37 CFR 1.312 has been considered, and has been:
- a) entered.
 - b) entered as directed to matters of form not affecting the scope of the invention.
 - c) disapproved because the amendment was filed after the payment of the issue fee.
Any amendment filed after the date the issue fee is paid must be accompanied by a petition under 37 CFR 1.313(c)(1) and the required fee to withdraw the application from issue.
 - d) disapproved. See explanation below.
 - e) entered in part. See explanation below.

/JOSEPH P. HIRL/ Supervisory Patent Examiner, Art Unit 2435	/Thomas Gyorfi/ Examiner, Art Unit 2435
--	--

Receipt date: 06/26/2007

Application Number

11768729 - GAU: 2435

Filing Date

2007-06-26

First Named Inventor

Kenneth P. Weiss

Art Unit

Examiner Name

Not Yet Known

Attorney Docket Number

W0537-700620

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Not for submission under 37 CFR 1.99)

Change(s) applied to document,

/A.G./

4/1/2014

	9	6516315	B1	2003-02-04	Gupta	
	10	6546005	B1	2003-04-08	Berkley et al	
	11	6581059	B1	2003-07-17 June 17, 2003	Barrett et al.	
	12	6640211	B1	2003-10-28	Holden	
	13	6658400	B2	2003-12-02	Perell et al.	
	14	6845448	B1	2005-01-18	Chaganti et al.	
	15	6941271	B1	2005-09-06	Soong	
	16	5058161		1991-10-15	Weiss	
	17	5168520		1992-12-01	Weiss	
	18	5657388		1997-08-12	Weiss	
	19	6393421		2002-05-21	Paglin	

Receipt date: 06/26/2007

11768729, CAU: 2435

Approved for use through 09/30/2007. OMB 0651-0031

U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

INFORMATION DISCLOSURE STATEMENT BY APPLICANT (Not for submission under 37 CFR 1.99)	Application Number		
	Filing Date		2007-06-26
	First Named Inventor	Kenneth P. Weiss	
	Art Unit		
	Examiner Name	Not Yet Known	
	Attorney Docket Number	W0537-700620	

Change(s) applied
to document,

/AG/

4/1/2014

U.S. PATENTS							Remove
Examiner Initial*	Cite No	Patent Number	Kind Code ¹	Issue Date	Name of Patentee or Applicant of cited Document	Pages, Columns, Lines where Relevant Passages or Relevant Figures Appear	
	1	5664109		1997-09-02	Johnson, et al.		
	2	5813006		1998-09-22	Polnerow et al.		
	3	6073106		2000-06-06	Rozen et al.		
	4	62532002 6,253,202	B1	2001-06-26	Gilmour		
	5	6253203	B1	2001-06-26	O'Flaherty et al.		
	6	6260039	B1	2001-07-10	Schneck et al.		
	7	6308203	B1	2001-10-23	Itabashi et al.		
	8	6393421	B1	2002-05-21	Paglin		

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /BD/



APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
11/768,729	10/07/2014	8856539	W0537-700620	3536

37462 7590 09/17/2014
LANDO & ANASTASI, LLP
ONE MAIN STREET, SUITE 1100
CAMBRIDGE, MA 02142

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment is 221 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Application Assistance Unit (AAU) of the Office of Data Management (ODM) at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional applicants):

Kenneth P. Weiss, Newton, MA;

The United States represents the largest, most dynamic marketplace in the world and is an unparalleled location for business investment, innovation, and commercialization of new technologies. The USA offers tremendous resources and advantages for those who invest and manufacture goods here. Through SelectUSA, our nation works to encourage and facilitate business investment. To learn more about why the USA is the best country in the world to develop technology, manufacture products, and grow your business, visit SelectUSA.gov.