

PROVISIONAL APPLICATION COVER SHEET

This is a request for filing a PROVISIONAL APPLICATION under 37 CFR 1.53(c).

DOCKET NUMBER: W0537-700900
Express Mail Label No. EV 307785964 US
Date of Deposit: February 21, 2006

113268 U.S. PTO
60/775046

INVENTOR(S)/APPLICANT(S)

Given Name (first and middle [if any])	Family Name or Surname	Residence (City and either State or Foreign Country)
Kenneth P.	Weiss	Newton, MA

TITLE OF THE INVENTION (500 characters max)

METHOD AND APPARATUS FOR EMULATING A MAGNETIC STRIPE READABLE CARD

CORRESPONDENCE ADDRESS

CUSTOMER NUMBER: 37462

ENCLOSED APPLICATION PARTS (check all that apply)

- Specification *Number of Pages* 22
- Drawing(s) *Number of Sheets* 3
- Application Data Sheet, See 37 CFR 1.76
- Return receipt postcard
- Other (specify): 1. Exhibit A (US Publication No. 2004/0133787) (35 pages)
2. Exhibit B (US Application No. 09/810,703) (48 pages)

The invention was made by an agency of the United States Government or under a contract with an agency of the United States Government.

No

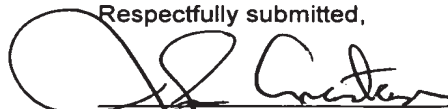
Yes, the name of the U.S. Government Agency and the Government Contract Number are:

METHOD OF PAYMENT (check all that apply)

- A check is enclosed to cover the Provisional Filing Fees, including the **Application Size Fee** (if applicable).
- The Commissioner is hereby authorized to charge any deficiencies or credit overpayment to Deposit Account 50/2762, Docket No. W0537-700900. A duplicate of this sheet is enclosed.
- Small Entity Status is claimed.

PROVISIONAL FILING FEE AMOUNT \$ 225.00

Respectfully submitted,


John N. Anastasi, Reg. No. 37,765
Telephone No.: 617-395-7000

February 21, 2006
Date

**METHOD AND APPARATUS FOR EMULATING A MAGNETIC STRIPE
READABLE CARD**

BACKGROUND OF INVENTION

1. Field of Invention

The invention relates generally to systems and methods for obtaining information from and/or transmitting information to a user device and, in particular, to systems, methods, and apparatus that provide for contactless information transmission.

2. Background

Today, both commercial (e.g., banking networks) and non-commercial (e.g., security systems) information systems often rely on magnetic card readers to collect information specific to a user (e.g., a security code, a credit card number, etc.) from a user device (e.g., a transaction card). Credit card purchases made in person provide an example of the most common transaction-type that relies on a user device, the credit or debit card, which is read by a magnetic card reader. User devices that rely on magnetic-stripe based technology magnetically store information (e.g., binary information) in the magnetic stripe. The magnetic stripe reader provides an interface to a larger computerized network that receives the user's information to determine, for example, whether to authorize a transaction, to allow the user access to a secure area, etc.

Recently, such devices have seen technological advances that increase their capabilities and improve their security. For example, such devices may now include embedded processors, integral biometric sensors that sense one or more biometric feature (e.g., a fingerprint) of the user, and magnetic stripe emulators. As one result, today's user devices may provide greater security by dynamically generating the necessary information, for example, generating the credit card number at the time of a transaction. Improved security can also be provided by such devices because more sophisticated authentication schemes can be implemented with the devices.

In addition, user devices such as transaction cards may now also provide for one or more modes of information transmission other than transmission via a magnetic stripe/card reader combination. For example, user devices that may transmit information optically or via radio frequency (“RF”) signal transmission to a compatible system interface are now available. Further, the architecture of a user device that includes a processor is generally compatible with both the improved security features described above and the contactless transmission modes such as optical and RF signal transmission. As a result of the improved security and greater functionality of some current user devices, there is a desire to replace magnetic-stripe based user devices with devices that include forms of information transmission other than the reading of a magnetic-stripe.

There is, however, a substantial installed base of interfaces (for example, at points of sale, at automatic teller machines (“ATM”), and the like) that include magnetic card readers which are not equipped to receive information from a user device in any other format other than from a magnetic stripe. As a result of the cost to replace or retrofit the installed base, efforts to more-widely introduce user devices that do not employ magnetic stripe devices have not been developed. Because of the potential to substantially reduce fraud, however, the further implementation of such devices is of great interest to financial institutions among others. RF devices that transmit information wirelessly are expected to become much more prevalent and at some point, the predominant form of information transmission for user authentication based on a hand-held device, for example, credit card, debit card, drivers license, passport, social security card, personal identification, etc. Thus, new and improved methods for transitioning from a purely magnetic based form of communication to a wireless form of communication are desired.

One current approach that is intended to “transform” a smart card for use with a magnetic stripe card reader employs a “bridge” device. The bridge device requires that the smart card be inserted within it. The bridge device includes a slot for receiving the smart card, a key pad whereby the user may enter information (e.g., a PIN number), and a credit card sized extension member. Operation of the bridge device requires that the smart card be inserted within it and that an electrical contact

surface of the smart card engage a similar surface within the bridge device before the bridge device (i.e., the extension member) can be used with a magnetic card reader. Thus, the contactless nature of more advanced information transmission systems is lost with the bridge device because it does not support wireless signal transmission.

SUMMARY OF INVENTION

In one aspect of the invention, a device converts a wireless transaction device to a magnetic-stripe emulator device. In one embodiment, the device includes a wireless signal receiver that is configured to receive a wireless signal and provide information from the wireless signal. In addition, the device may include a magnetic-stripe emulator which is communicatively coupled to the wireless signal receiver and adapted to provide a time-varying signal which emulates data provided by a magnetic-stripe card to a magnetic card reader in response to receiving the information from the wireless signal. In one embodiment, the device includes a processor communicatively coupled to the wireless signal receiver and to the magnetic-stripe emulator. The device may also include an LED. In a version of this embodiment, the processor is configured to control the LED to indicate that the device is properly aligned with the magnetic card reader. In another embodiment, the device includes an output device that can provide information to a network or to a network device. In a version of this embodiment, the output device is a wireless transmitter device.

Further embodiments of the invention may include additional features, for example, in one embodiment the output device is a data port to which the device can provide data to a network or to a network device. In a version of this embodiment, the data port is also configured to receive data from the network or the network's device. In a further embodiment, the device is configured to communicate with the magnetic card reader via the data port.

In a further embodiment, the wireless receiver and/or processors configure, decrypt and encrypt the wireless signal. In a further embodiment, the processor is configured to determine whether a user is authorized to provide the information contained within the wireless signal from data within the wireless signal. In a version of this embodiment, the data contained within the wireless signal includes user ID

information. In yet another embodiment, the data contained within the wireless signal includes biometric information of the user.

BRIEF DESCRIPTION OF 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 illustrates a system in accordance with one embodiment of the invention;

FIG. 2 illustrates a process in accordance with an embodiment of the invention; and

FIGS. 3A-3D illustrate a converter device in accordance with one embodiment of the invention.

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 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.

FIG. 1 illustrates an embodiment of a system 100 that employs a converter device 102 to provide an interface between a user device 104 (e.g., a transaction card) and a system interface 106 where, for example, the system interface 106 employs a magnetic card reader and the user device 104 is not equipped with a magnetic stripe. That is, in one embodiment, the converter device 102 provides a mode of information transmission between the user device 102 and the system interface 106 which would otherwise be unavailable to the user device 102. The converter device 102 provides a

modified system 100 that provides compatibility with a greater variety of user devices, for example, user devices such as transaction cards that are not equipped with a magnetic stripe. For example, in one embodiment, the converter device 102 includes a magnetic stripe emulator 137 communicatively coupled to a wireless signal receiver 140 and adapted to provide a time-varying signal emulating data provided by a magnetic stripe card to a magnetic card reader 152.

The user device need not be a "card" and may, for example, take the form of a fob used as a key ring, a cell phone, a watch, a personal digital assistant or any device that can include a wireless transmitter, or a magnetic stripe emulator.

In general, the system interface 106 provides an interface to a larger information system (e.g., a financial system, an access control system, a medical records system, and the like) that in one embodiment includes a system processor or controller 110, a database 112, a network 114, other systems 116, such as a universal secure registry 118 as will be described further herein. Each of the preceding system elements may be placed in communication with any one or any combination of the system elements, for example, over communication links 120A, 120B, 120C, 120D. It should be recognized that the communication links 120 need not provide the communication paths shown in FIG. 1 and that other communication paths may be employed. For example, the database 112 may be connected to the network 114 via the communication link 120A and to the system processor 110 via the communication link 120B instead of being connected as shown in FIG. 1.

The communication link may be a wireless communication link, a hardwired communication link, a fiber optic communication link, any communication link used in the art, as well as a combination of any of the preceding or any other any communication link capable of transmitting signals between the elements of the system 100. The system processor 110 allows information transfer of both data and instructions, for example, between the interface 106 and one or more databases which may be connected to the system or other network elements.

In general, the operation of the converter device 102 allows a user in possession of a transaction card 104 to wirelessly communicate information to the device so that the device can be employed to interface with a network system. For

example, in one embodiment, the network system may provide a magnetic card reader interface and the converter device 102 provides a magnetic stripe emulator that can interface with the system. In general, the overall operation of the system 100 includes the communication of information between the user device 104 and the converter device 102, for example, RF communication. In one embodiment, the communication is bi-directional such that information can be communicated both to and from the user device 104. The converter device 102 provides an interface by which information derived from the information being transmitted to or from the user device 104 is transmitted between the converter device and the system interface 106. The system interface 106 provides the communication interface between it and the remainder of the system 100 (e.g., processor 110, database 112, network 114, etc.).

According to one embodiment, the user device 104 includes a processor 122, a user interface 124, a wireless transmitter 126 and card indicia 128. In another embodiment, the user device 104 includes a biometric sensor 130. In various embodiments, the processor 122 is communicatively coupled to each of the wireless transmitter 126, the user interface 124 and the biometric sensor 130.

The processor 122 may include a chip such as a general purpose processor, an application specific integrated circuit (“ASIC”), or a field programmable gate array (“FPGA”) and the like that may execute various programs and/or provide logic inputs and outputs. For example, the processor 122 may process biometric information received from the biometric sensor 130 to verify the identity of the user before the user can employ the user device 104. Exemplary details of a processor and biometric sensor which are configured to authenticate a fingerprint of a user are disclosed in U.S. published application 2004/0133787, published on July 8, 2004, which is herein incorporated by reference and also attached as Exhibit A. The processor 122 may also include or be coupled to driver circuitry to drive a display included in the user interface 124 and can be configured to process user input data entered via the user interface 124. In one embodiment, the user interface 124 includes one or more control inputs (for example, control buttons).

The wireless transmitter 126 can process information provided by the processor and convert the information to an RF signal and can also include an RF

antenna that transmits the RF information wirelessly. In another embodiment, the transaction card may also include an RF receiver that receives a wireless RF signal from the RF antenna and converts the RF signal to an information signal provided to the processor. It is to be appreciated that the wireless transmitter and/or receiver need not be an RF device, it can also be any of a IR device, an optical device, a Bluetooth signal or any other wireless signal transmitter or receiver used in the art.

The user device may also include a power source such as a battery that fits within the device. In one alternative embodiment, the user device remains in a sleep mode until it is placed in the vicinity of an RF transmitter at which time the user device 104 converts received RF energy into electrical energy used to provide power to the processor 122 and the other components included in the user device 104.

According to one embodiment, the user device 104 can be a smart card configured for wireless signal transmission using RF signals. For example, the wireless transmitter 126 may be an RF transmitter device or any other wireless transmitter device configured to transmit the smart card information of the card. Alternatively, it is to be appreciated that the card can be many cards such as a debit card, a plurality of credit cards such as VISA, MasterCard, American Express, or any other card with the card indicia and relevant information being stored in card memory 129 and read out by processor 122 and provided to the wireless transmitter 126.

In the embodiment illustrated in FIG. 1, the converter device 102 includes a substrate 132 which may include a stripe 134 and a magnetic field generator 136 which together comprise the magnetic stripe emulator 137, a processor 138, a wireless receiver 140, a user interface 142, a memory 144, and a power source 146. In a further embodiment, the converter device 102 includes an indicating light 148 (e.g., an LED) and an output device 150.

According to one embodiment, the system interface 106 with which the converter device 132 is employed includes any of or all of a magnetic card reader 152, a wireless transceiver 154 and a data port 156.

In general, according to one embodiment, the converter device 102 receives a wireless signal from the user device 104, processes the information that is received and provides an output in the form of a time-varying signal provided to the stripe 134

(e.g., a magnetic stripe). The signal provided to the stripe 134 can then be provided to the system processor 110 by inserting the stripe and the associated substrate 132 or portion thereof in the magnetic card reader of the system interface 106. That is, in one embodiment, the stripe 134 and at least a portion of the substrate 132 can be either slid by the magnetic card reader 152 or inserted to sit statically in front of the read head of the card reader.

The processor 138 may be a general purpose processor, an application specific integrated circuit (“ASIC”), or a field programmable gate array (“FPGA”) and may be implemented in hardware, software, firmware or any combination of the preceding. The processor 138 may be communicatively coupled with any of the magnetic field generator 136 the wireless receiver 140, the memory 144, the user interface 142, the light source 148, the power source 146 and the output device 150. In general, the processor can be configured to receive inputs from one or more of the preceding elements and may provide outputs to each of the elements included in converter device 138.

For example, according to one embodiment, the magnetic stripe 134 is a programmable magnetic stripe and the magnetic field generator 136 generates a magnetic signal that controls the information provided by the magnetic stripe 134. The U.S. Patent Application No. 10/680,050, filed October 7, 2003, entitled “System Method and Apparatus for Enabling Transactions Using a Biometrically Enabled Programmable Magnetic Stripe which was published on July 8, 2004 as US2004/0133787 (the ‘050 application), provides further details concerning embodiments of a transaction card that emulates a magnetic stripe and may also include, for example, a biometric sensor. The ‘050 application is attached hereto as Exhibit A. In this embodiment, the processor 138 may control the operation of the magnetic field generator 136 to provide the desired information to the stripe 134. For example, the processor 138 may provide an output to the stripe 134 in response to receiving information from the wireless receiver 140, where the information from the wireless receiver is information transmitted from the user device 104.

Further, the processor 138 may be configured to provide signals to drive a display included in the user interface 142 and process user input data entered with the

user interface 142. In one embodiment, the user interface 142 includes a display screen that can be used to display an image of the user to whom the user device 104 belongs, for security purposes. The image to be displayed by the UI can either be part of the information transmitted by the transaction card 104, for example, where the transaction card 104 also requires some authentication by the user before transmitting the card information and image, or can be provided, for example, by the USR system 118 through the system interface 106 as part of the user authentication process, as will be described in more detail herein. In further embodiments, the user interface 142 may include a plurality of control elements that allow the user and/or the transaction processor (e.g., store clerk, security guard, medical service provider, etc.) to enter information into the converter device 102.

The processor 138 may also be configured to provide signals to operate the indicating light 148. The indicating light 148 may provide an indication of the operational status of the converter device 102, for example, the indicating light 148 may indicate any of the following: that the converter device 102 is receiving a transmission from a user device 104; that the converter device 102 has generated output data to the stripe 134; the status of the power source 146 is normal or conversely that the power source has a low power level; that the converter device 102 is transmitting information via the output device 150; that the converter device 102 is properly aligned with the magnetic card reader 152; that the converter device 102 has received authorization for a transaction; and the like. It should be apparent to one of skill in the art that the indicating light may be a single lamp or a plurality of lamps and that the lamp or lamps may be a single color including white or may included a plurality of colors. Further, it should also be apparent that the lights may provide a plurality of status indications based on their color, intensity, rate of change of the preceding characteristics or any combination of these and other features.

The power source 146 may include a battery power source or other energy sources suitable for the form factor of the converter device 102. For example, in a form factor where the converter device 102 is a hand-held device the power source 146 may be any one of a standard size battery (e.g., a AA battery). In a further embodiment, the power source is a lithium battery. Alternatively, the power source

can be any of an AC power source, an AC to DC converter device, or any other DC power source known to those skilled in the art.

According to one embodiment, the converter device 102 includes a power bus 158 that provides a path for the transmission of power to the various components included in the converter device 102.

In accordance with one embodiment, the converter device 102 includes the output device 150. It is to be appreciated that the output device can be any standard interface device to be coupled to a data bus such as a USB device, or the output device can be configured for contactless communication with the system interface 106. For example, in one embodiment, the output device is an optical transmitter device. In general, the communication between the converter device 102 and the system interface 106 is bi-directional such that information (e.g., information associated with the user's identity) may be transmitted to the system interface 106, the system processor 110 may generate a response (e.g., a transaction approval), and the response may be transmitted to the converter device 102 via the system interface 106.

In one embodiment, the processor 138 is configured in combination with the output device 150 to provide an encrypted output signal. In a further embodiment, the processor 138 is configured in combination with the output device 150 to provide a time-varying encrypted output signal. In yet another embodiment, the processor 138 is configured in combination with the output device 150 to provide a time-varying encrypted (or not) public and private key output signal. In addition, the processor can also be configured in combination with the wireless receiver to receive and decrypt any and all of an encrypted signal, a time-varying encrypted signal and a time-varying encrypted (or not) public and private key as provided by the transaction card 104.

In some embodiments, the output device 150 need not transmit any personal information associated with the user. For example, commonly owned U.S. Patent Application No. 09/810,703, filed March 16, 2001, entitled "Universal Secure Registry" ("the '703 application") describes an approach that can improve security and reduce the need for multiple forms of identification. The '703 application is herein attached as Exhibit B and is incorporated herein by reference in its entirety. The universal secure registry 118 included in the system 100 provides one example of

the integration of such a registry into a system that employs a converter device 102. With the USR system, for example, the transaction card 104 can provide some information, e.g., such as a public code of the user, which can be authenticated by the user, for example by providing an ID through the user interface 124 or through biometric sensor 130. The public code can be provided to the USR via the converter 102, system interface 104, and network 114. The USR can then provide back to any of the system interface and the converter device any or all of transaction card information, authorization for a transaction, e.g., where the network or the USR also communicates with the relevant authority, and indicia about the card holder. Various alternatives and embodiments are described in the attached Exhibit B.

The system 100 may include a variety of system interfaces 106 of different types such as the wireless transceiver 154 and the data port 156 in addition to the magnetic card reader 152. Although not illustrated, other system interfaces such as an optical interface, a smart card reader interface or any other system interface known to those of skill in the art can also be included. Further, the system interfaces may be either commonly located or may be geographically distributed such that some locations include a wireless transceiver 154, some locations include a data port 156, some locations include a magnetic card reader 152, and some locations include a plurality of types of system interfaces.

Thus, in some embodiments the output device 150 of the converter device 102 may include a data port via which the converter device 102 can provide data to a network or a networked device. In one embodiment, the data port is also configured to receive data from the network or a networked device.

Embodiments of the converter device 102 can be configured to provide communication to the system interface 106 via any of the preceding approaches including wireless signal transmission. In a version of this embodiment, the converter device 102 may receive wireless signals from the user's transaction card and transmit wireless signals to the system interface 106. Further, the device may include a transmitter that allows it to transmit information back to the user's transaction card.

Referring now to FIG. 2, a process 260 employing the converter device 102 is illustrated in accordance with one embodiment. The process begins at Stage 262 –

START. Here, the converter device 102 is in a steady state in which it awaits receipt of a signal from a user device 104. At Stage 264, the converter device 102 receives data, for example, a wireless signal transmitted from the user device 104. At Stage 266, the converter device 266 extracts information from the wireless signal for processing. As one example, the converter device 102 may extract information corresponding to the user's identity and/or the identity of the individual to whom the user device was issued. The extracted information is then provided to the system interface, for example, it is simulated as magnetic striped data to the magnetic card reader. At Stage 268, the system 100 authenticates the user. In one embodiment, if the authentication is successful, the process continues at Stage 270. In this embodiment, if the authentication is unsuccessful, the process returns to Stage 262 where, for example, the user may be prompted to attempt to authenticate again.

Various user authentication approaches may be implemented using the converter device 102. For example, the authentication may be performed locally, that is, without the need for communication between the converter device 102 and the system interface 106 and system processor 110. In one embodiment, the authentication process employs the universal secure registry 118. In further embodiments, the authentication process employs one or more authentication protocols such as public-key cryptography, key exchange protocols, protocols employing one-way functions, and the like that are well known by those of ordinary skill in the art. In other embodiments, however, the authentication may require an exchange of information between the converter device 102 and any of the system interface 106, the network 114, the USR 118 and another database 112.

At Stage 270, the completion of the transaction may be involve any of a wide variety of acts including: authorizing a withdrawal of money from a user's account, permitting the user access to a secure area, permitting a user to view medical information concerning themselves or a third party, or permitting the user to access other confidential information.

In addition, in some embodiments, the process 260 includes Stage 274 where following authentication the converter device 102 receives information associated with the user. The information may, for example, be necessary for the completion of

the transaction. For example, where the system 100 is employed in conjunction with a check-authorization process, the converter device 102 may receive an indication that the user has sufficient funds to cover the amount of the check that is presented at a point of sale. Alternatively, or in addition, the information may include indicia related to the authorized holder of the transaction card 104, such as a picture ID, as is described in more detail in the attached Exhibit B. The process 260 is completed at Stage 272 – END.

An embodiment, of the converter device 302 is illustrated in FIGS. 3A through 3D. As illustrated in the front view of FIG. 3A, in one embodiment, the converter device 302 includes a housing 380, a substrate 332, and a magnetic stripe 334. In one embodiment, the housing 380 is manufactured from a rigid material, for example, metal or plastic and the converter device 302 is designed to be a hand-held device. FIG. 3B illustrates a side view perspective of an embodiment of the converter device 302, showing an indicating light 348 (e.g., an LED). As described in greater detail above, the indicating light 348 can include a single indicating light or a plurality of indicating lights.

FIGS. 3A-3D illustrate an embodiment where the substrate extends substantially perpendicular from a side of the housing 380, however, the specific angle at which the substrate extends from the housing may vary so long as the housing does not interfere with the insertion of the substrate into, for example, the magnetic card reader 152.

FIG. 3D illustrates a top view of an embodiment of the converter device 302 which includes a display screen (e.g., an LCD display screen) that may provide the user interface 342 or a portion of the user interface of the converter device 302. In one embodiment, the user interface 342 includes a display screen that displays either a black and white or a color image of the individual to whom the user device 104 was issued. It should be recognized that the display screen may provide a wide range of functionality, for example, the display screen may display a variety of data received by the converter device 302 including data represented in alpha numeric format.

The magnetic stripe 334 may be a programmable magnetic stripe such that the converter device 302 provides a magnetic stripe emulator. In one embodiment, as has

been described herein, the converter device 302 receives a wireless signal from a user device 102 and provides a time varying signal which emulates data provided by a magnetic-stripe card to a magnetic card reader in response to receiving the information from the wireless signal. In a further embodiment, the information is provided to the magnetic card reader by inserting the magnetic stripe 334 into the magnetic card reader.

The various embodiments of a system and method for converting a wireless transaction device to a magnetic stripe emulator device may include any of the following or any combination of the following: a converter device with a processor communicatively coupled to a wireless signal receiver and to a magnetic stripe emulator. The converter device may optionally include an LED. Further the processor may be configured for any combination of the following: control of the LED to indicate that the device is properly aligned with the magnetic card reader, control of the LED to indicate that the device has received authorization for a transaction, and where the converter device includes a power supply, a processor configured to control the LED to indicate that the device has power.

In one embodiment, the information received from the wireless signal by the converter device may include any of a name, a card number, user identification, a device code, amount of credit available, and an expiration date of the card for a transaction.

Further, in various embodiments, the converter device may include an output device that can provide information to a network or to a networked device. In various embodiments, the output device can be configured as a wireless transmitter device, such as an optical transmitter device.

In various embodiments the wireless transmitter device where the wireless transmitter may generally be configured as an RF transmitter device, and in particular, as a Bluetooth transmitter device.

In addition, in various embodiments, the processor can be configured in combination with the output device to provide any of an encrypted output signal, a time-varying encrypted output signal, and in particular, a time-varying public and private key output signal.

In further embodiments, the converter device may include an output device configured as a data port via which the converter device can provide data to a network or a networked device and to receive data from the network or a networked device.

In one embodiment, the converter device may also include an LCD screen for displaying at least some of the data received by the converter device, and a processor configured in combination with the LCD device to display indicia corresponding to the authorization of a transaction, and in particular, indicia that includes picture information of the cardholder.

In addition to the above described features, the various embodiments of a system and method for converting a wireless transaction device to a magnetic stripe emulator device may include any combination of the following or any combination of the following and the above listed features: the converter device can be configured to communicate with the magnetic card reader via the data port; the wireless receiver and/or processor is configured to decrypt an encrypted wireless signal; the converter device is configured to decrypt a time-varying encrypted wireless signal; the converter device configured to decrypt time-varying public and private key information contained within the wireless signal; the converter device includes a user interface communicatively coupled to the processor; the converter device processor is configured to determine whether the user is authorized to provide the information contained within the wireless signal from data provided through the user interface.

In addition, the following further additional features may be combined alone or in combination with the preceding: the data contained within the wireless signal received by the converter device may include any combination of the following: user I.D. information, biometric information of the user, secret information, (for example, a PIN, a password, or a passcode of the user), or information about an uncounterfeitable token of the user.

In various embodiments, the converter device may include a substrate housing the magnetic stripe emulator, and the substrate may include a programmable magnetic stripe.

In various embodiments, the system employed with the converter device may also include a system interface coupled to a network where the system interface

includes a magnetic stripe reading device configured to read a time-varying signal. In a further embodiments, the system interface may be configured to transmit data received from the wireless transaction device to a networked credit card authentication entity also coupled to the network. The system may also include any of a keyboard, a printer, an (LCD) display, and an audio signal transducer.

Although the preceding description is primarily directed to an embodiment of the user device 104 that does not include a magnetic stripe, it should be recognized that some embodiments of the user device 104 may include a magnetic stripe. In these various embodiments, the converter device 102 may be employed to convert information coded on the magnetic stripe for transmission via another mode of information transmission.

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. Accordingly, the foregoing description and drawings are by way of example only.

What is claimed is:

CLAIMS

1. A device for converting a wireless transaction device to a magnetic stripe emulator device, comprising:
 - a wireless signal receiver configured to receive a wireless signal and to provide information from the wireless signal;
 - a magnetic stripe emulator communicatively coupled to the wireless signal receiver and adapted to provide a time-varying signal emulating data provided by a magnetic stripe card to a magnetic card reader, in response to receiving the information from the wireless signal.
2. The device of claim 1, further comprising a processor communicatively coupled to the wireless signal receiver and to the magnetic stripe emulator.
3. The device of claim 2, wherein the information includes any of a name, a card number, user identification, a device code, amount of credit available, and an expiration date of the card for a transaction.
4. The device of claim 2, further comprising a LED.
5. The device of claim 4, wherein the processor is configured to control the LED to indicate that the device is properly aligned with the magnetic card reader.
6. The device of claim 4, wherein the processor is configured to control the LED to indicate that the device has received authorization for a transaction.
7. The device of claim 4, further comprising a power supply.
8. The device of claim 7, wherein the processor is configured to control the LED to indicate that the device has power.

9. The device of claims 1 or 2, further comprising an output device that can provide information to a network or to a networked device.
10. The device of claim 9, wherein the output device is a wireless transmitter device.
11. The device of claim 10, wherein the wireless transmitter device is an RF transmitter device.
12. The device of claim 10, wherein the wireless transmitter device is a Bluetooth transmitter device.
13. The device of claim 9, wherein the output device is an optical transmitter device.
14. The device of claim 9, wherein the processor is configured in combination with the output device to provide an encrypted output signal.
15. The device of claim 9, wherein the processor is configured in combination with the output device to provide a time-varying encrypted output signal.
16. The device of claim 9, wherein the processor is configured in combination with the output device to provide a time-varying public and private key output signal.
17. The device of claim 9, wherein the output device is a data port to which the device can provide data to a network or a networked device.
18. The device of claim 17, wherein the data port is also configured to receive data from the network or a networked device.

19. The device of claim 18, further comprising a LCD screen for displaying at least some of the data received.
20. The device of claim 19, wherein the processor is configured in combination with the LCD device to display indicia corresponding to the authorization of the transaction.
21. The device of claim 20, wherein the indicia includes picture information of the cardholder.
22. The device of claim 17, wherein the device is configured to communicate with the magnetic card reader via the data port.
23. The device of claim 17, wherein the data comprises any of a name, a card number, user identification, a device code, amount of credit available, and an expiration date of the card for a transaction.
24. The device of claims 1 or 2, wherein the wireless receiver and/or processor is configured to decrypt an encrypted wireless signal.
25. The device of claim 24, wherein the device is configured to decrypt a time-varying encrypted wireless signal.
26. The device of claim 24, wherein the device is configured to decrypt time-varying public and private key information contained within the wireless signal.
27. The device of claim 2, further comprising a user interface communicatively coupled to the processor.

28. The device of claim 27, wherein the processor is configured to determine whether the user is authorized to provide the information contained within the wireless signal from data provided through the user interface.
29. The device of claim 2, wherein the processor is configured to determine whether a user is authorized to provide the information contained within the wireless signal from data within the wireless signal.
30. The device of claim 29, wherein the data contained within the wireless signal comprises user I.D. information.
31. The device of claim 29, wherein the data contained within the wireless signal comprises biometric information of the user.
32. The device of claim 29, wherein the data contained within the wireless signal comprises any of secret information, a PIN, a password, or a passcode of the user.
33. The device of claim 29, wherein the data contained within the wireless signal comprises information about an uncounterfeitable token of the user.
34. The device of claim 1 or 2, further comprising a substrate housing the magnetic stripe emulator.
35. The device of claim 34, wherein the substrate comprises a programmable magnetic stripe.
36. The device of claim 2, wherein the processor is configured to provide binary data to the magnetic stripe emulator.

37. The device of claim 1 or 2, further comprising a system interface coupled to a network that includes a magnetic stripe reading device configured to read the time-varying signal.

38. The device of claim 37, further wherein the system interface is configured to transmit data received from the wireless transaction device to a networked credit card authentication entity also coupled to the network.

39. The device of claim 37 or 38, further comprising any of keyboard, printer, (LCD) display audio signal.

40. The device of claim 1 or 2, further comprising a system interface that is configured to transmit data received from the wireless transaction device to a networked credit card authentication entity also coupled to the network.

ABSTRACT

In one aspect of the invention, a device converts a wireless transaction device to a magnetic-stripe emulator device. In one embodiment, the device includes a wireless signal receiver that is configured to receive a wireless signal and provide information from the wireless signal. In addition, the device may include a magnetic-stripe emulator which is communicatively coupled to the wireless signal receiver and adapted to provide a time varying signal which emulates data provided by a magnetic-stripe card to a magnetic card reader in response to receiving the information from the wireless signal.

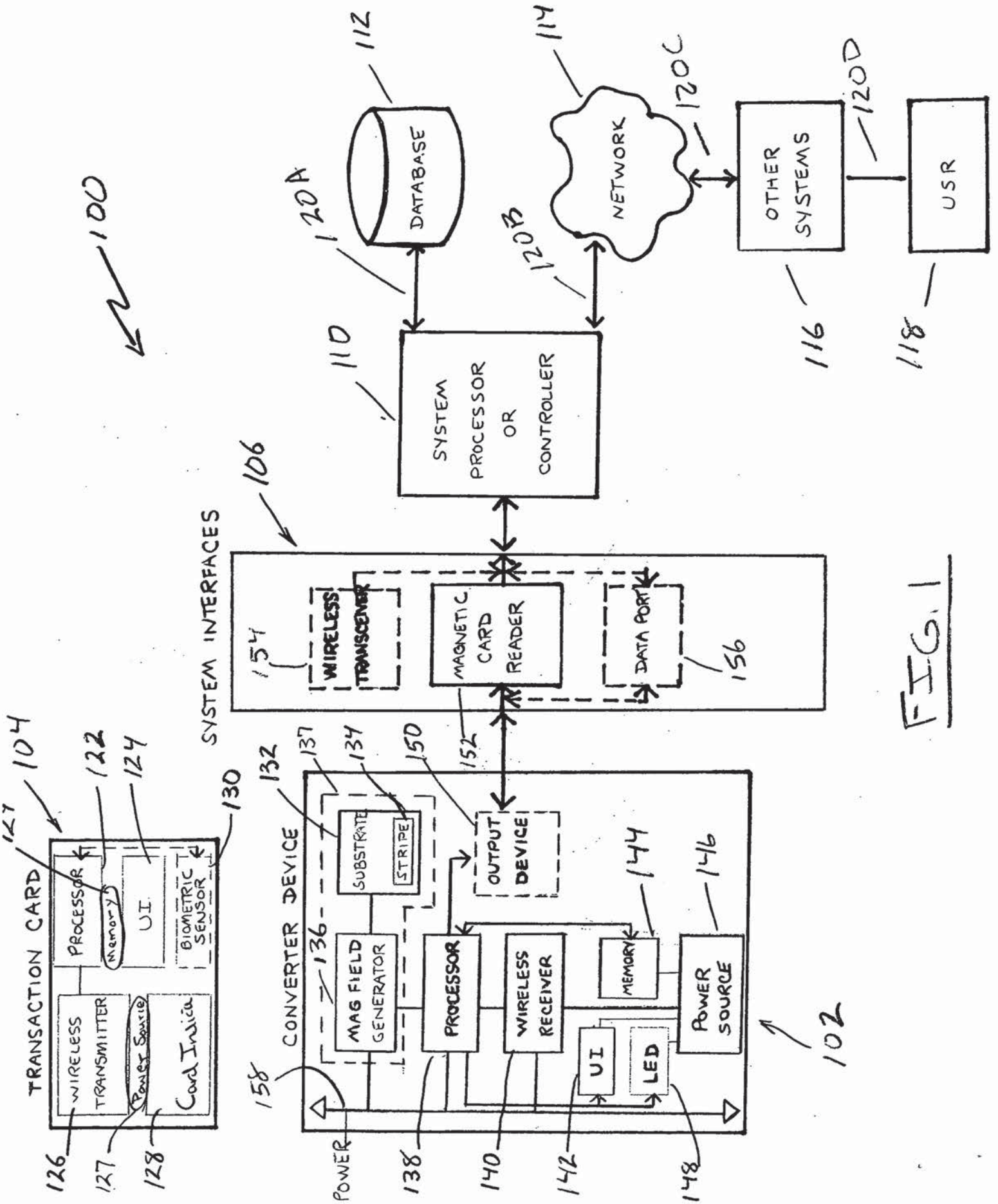


FIG. 1

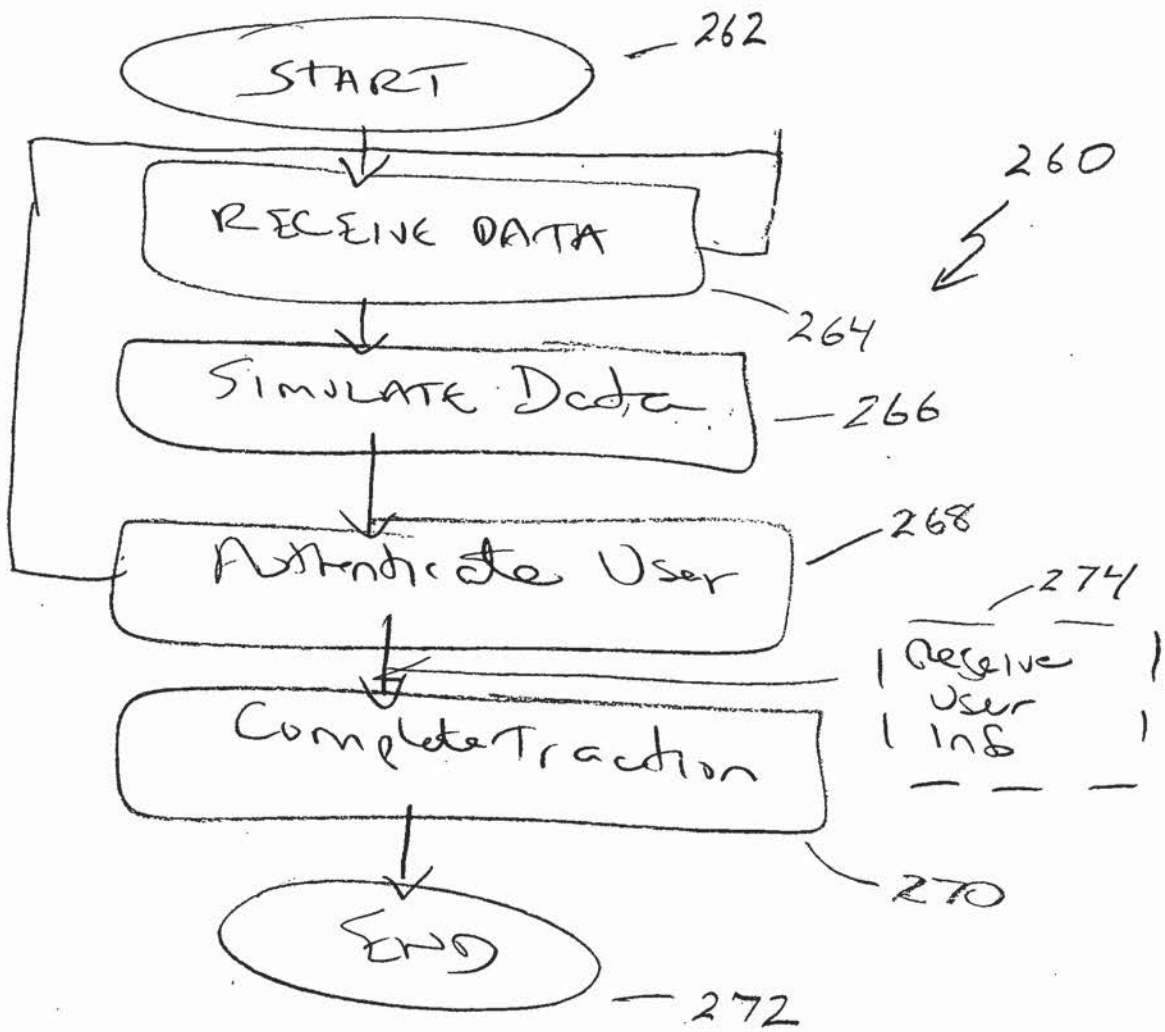
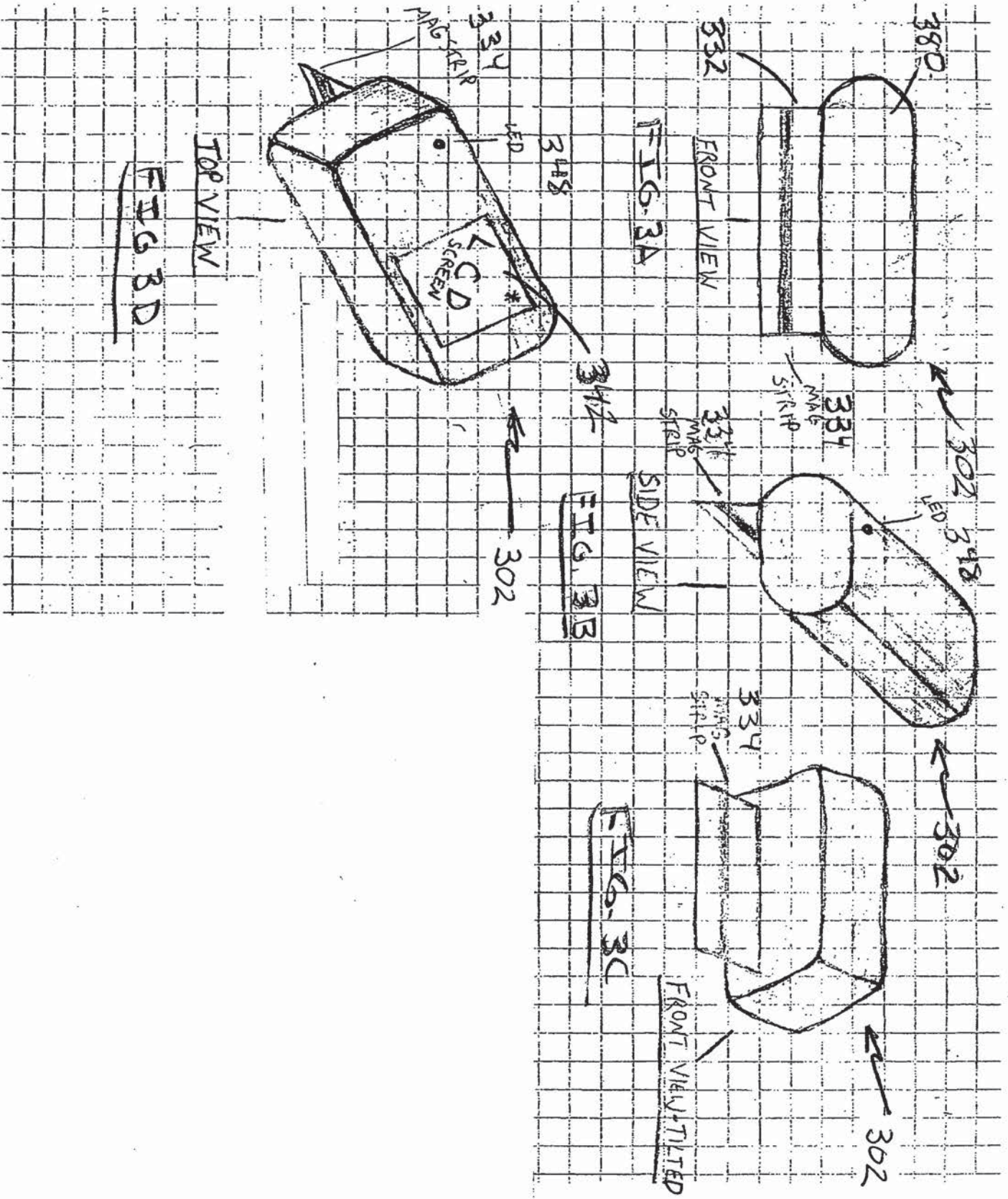


FIG. 2

Rest Available Copy



Best Available Copy

PATENT APPLICATION SERIAL NO. _____

U.S. DEPARTMENT OF COMMERCE
PATENT AND TRADEMARK OFFICE
FEE RECORD SHEET

02/23/2006 AKELECH1 00000097 60775046

01 FC:2005	100.00 OP
02 FC:2085	125.00 OP

PTO-1556

(5/87) :

U.S. Government Printing Office: 2002 — 489-267/88033

APPLICATION DATA SHEET

Application Information

Application Type::	Provisional
Subject Matter::	Utility
Title::	METHOD AND APPARATUS FOR EMULATING A MAGNETIC STRIPE READABLE CARD
Attorney Docket Number::	W0537-700900
Request for Early Publication?::	No
Request for Non-Publication?::	No
Suggested Drawing Figure::	1
Total Drawing Sheets::	3
Small Entity?::	Yes
Petition included?::	No
Secrecy Order in Patent Appl.?::	No

Applicant Information

Applicant Authority Type::	Inventor
Primary Citizenship Country::	US
Given Name::	Kenneth
Middle Name::	P.
Family Name::	Weiss
City of Residence::	Newton
State or Province of Residence::	MA
Country of Residence::	US
Street of mailing address::	49 Sargent Street
City of mailing address::	Newton
State or Province of mailing address::	MA
Country of mailing address::	US
Postal or Zip Code of mailing address::	02158

Attorney Docket No. W0537-700900
Page 2

Correspondence Information

Correspondence Customer Number:: 37462
Phone Number:: (617) 395-7000
Fax Number: (617) 395-7070

Representative Information

Representative Customer Number::	37462
----------------------------------	-------



US 20040133787A1

(19) **United States**

(12) **Patent Application Publication**
Doughty et al.

(10) **Pub. No.: US 2004/0133787 A1**

(43) **Pub. Date: Jul. 8, 2004**

(54) **SYSTEM, METHOD AND APPARATUS FOR ENABLING TRANSACTIONS USING A BIOMETRICALLY ENABLED PROGRAMMABLE MAGNETIC STRIPE**

(60) Provisional application No. 60/368,363, filed on Mar. 28, 2002.

Publication Classification

(75) Inventors: **Ralph O. Doughty**, Colleyville, TX (US); **Patrick R. Antaki**, Plano, TX (US)

(51) **Int. Cl.⁷** **H04L 9/00**
(52) **U.S. Cl.** **713/186**

(57) **ABSTRACT**

The present invention provides a system, method and apparatus that includes a user device having a magnetic field generator disposed within a substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate and a processor disposed within the substrate that is communicably coupled to the magnetic field generator, the biometric sensor and the memory. The processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified. A power source is also disposed within the substrate. The magnetic field generator can create a spatially varying magnetic signal using a magnetic stripe and one or more induction coils, or create a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader.

Correspondence Address:
CHALKER FLORES, LLP
12700 PARK CENTRAL, STE. 455
DALLAS, TX 75251 (US)

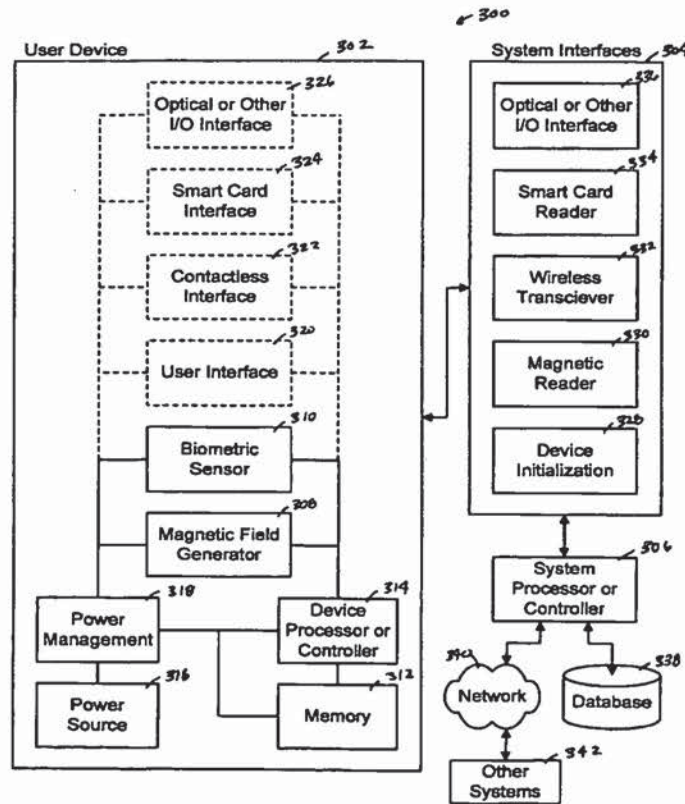
(73) Assignee: **Innovation Connection Corporation**, Richardson, TX (US)

(21) Appl. No.: **10/680,050**

(22) Filed: **Oct. 7, 2003**

Related U.S. Application Data

(63) Continuation-in-part of application No. 10/400,306, filed on Mar. 27, 2003.



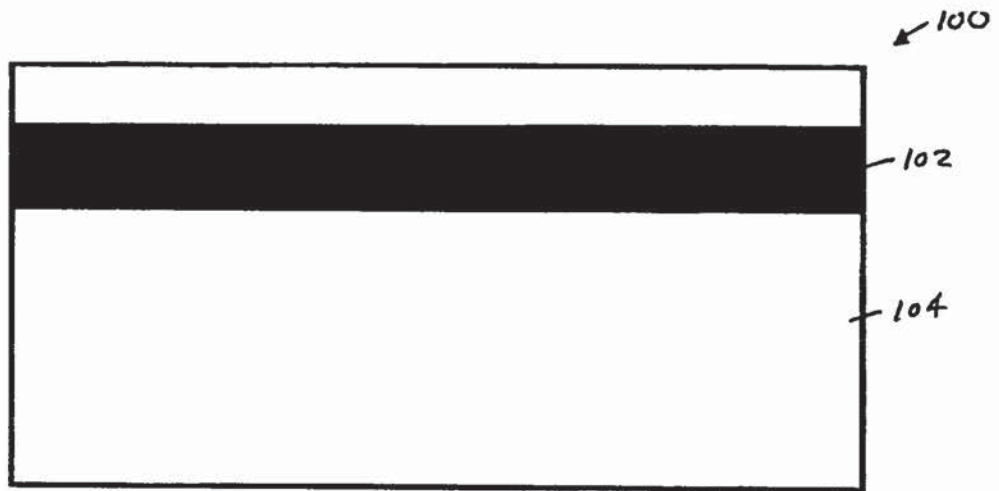


FIG. 1 (PRIOR ART)

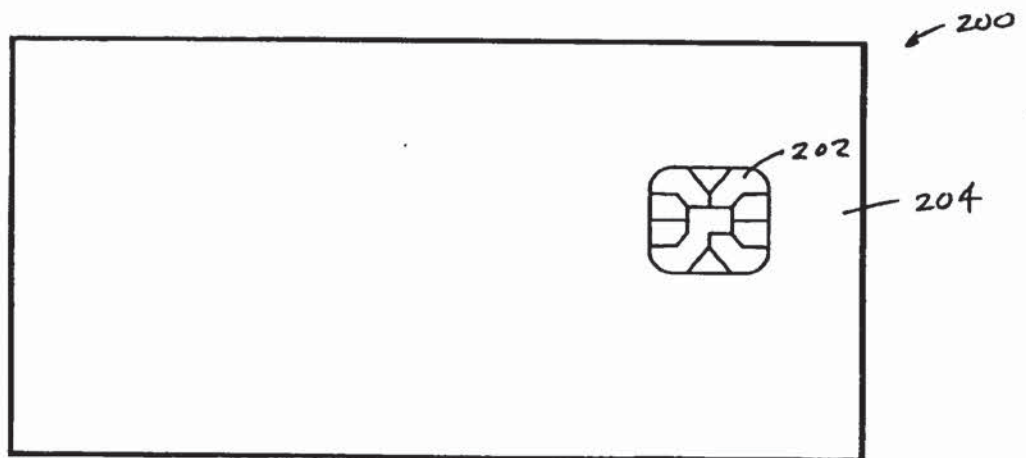


FIG. 2 (PRIOR ART)

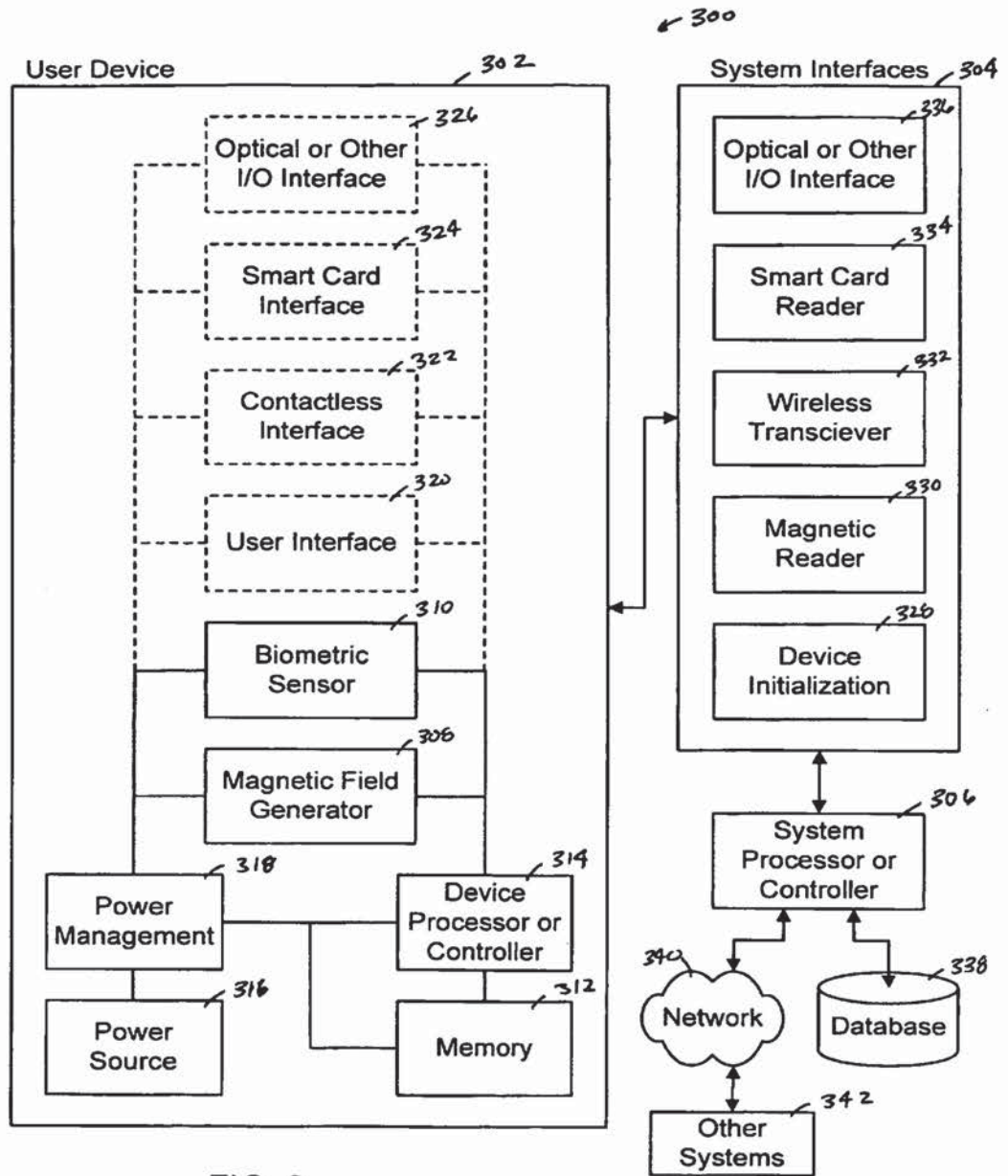


FIG. 3

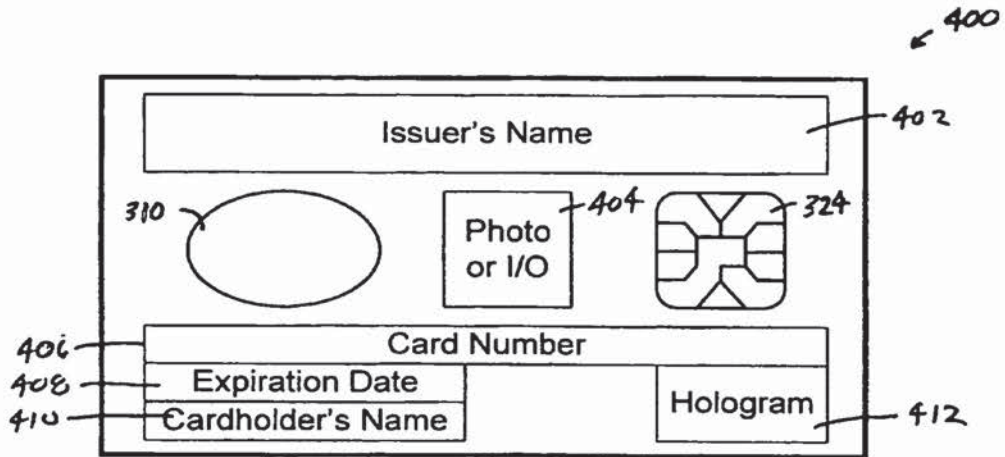


FIG. 4A

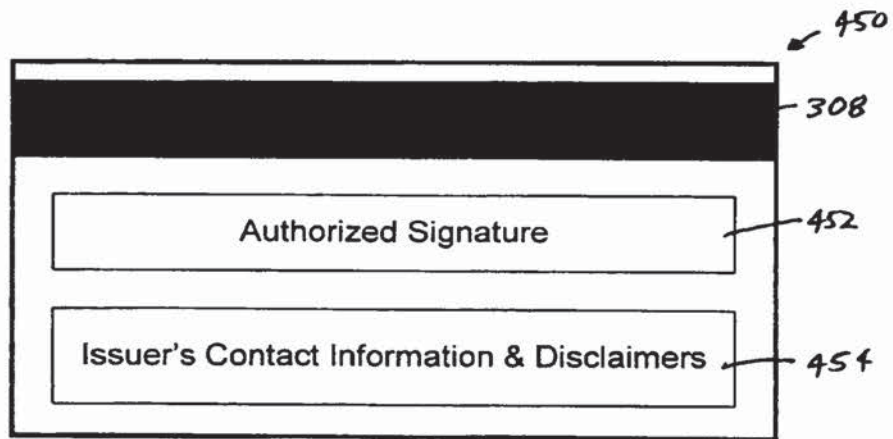


FIG. 4B

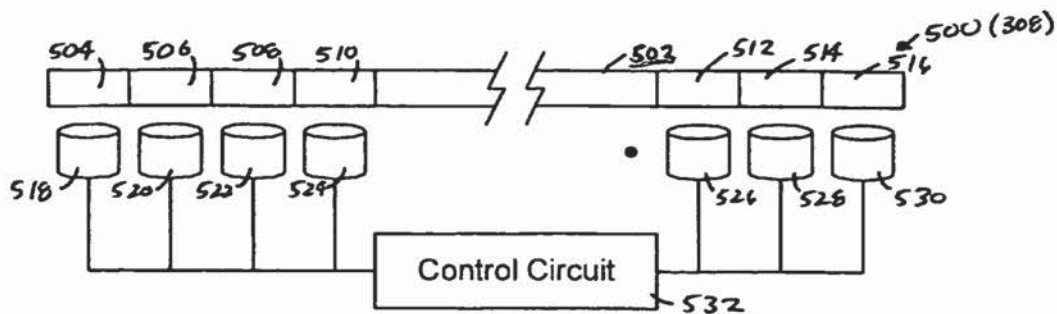


FIG. 5A

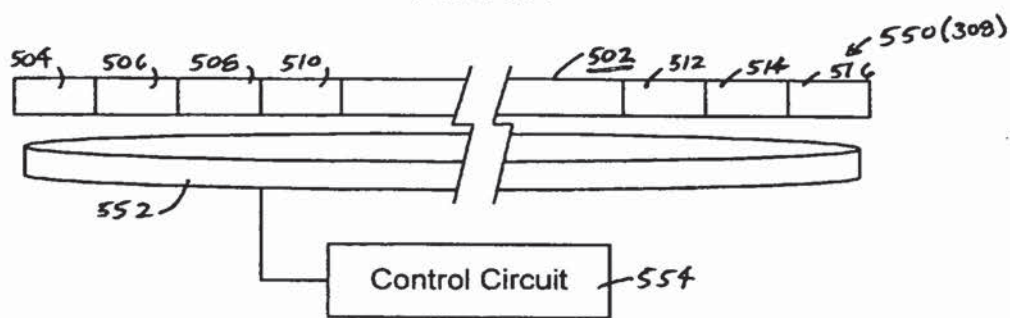


FIG. 5B

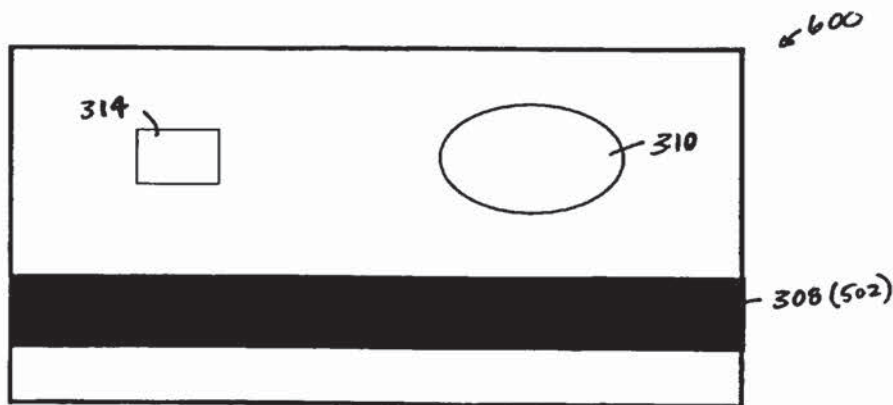
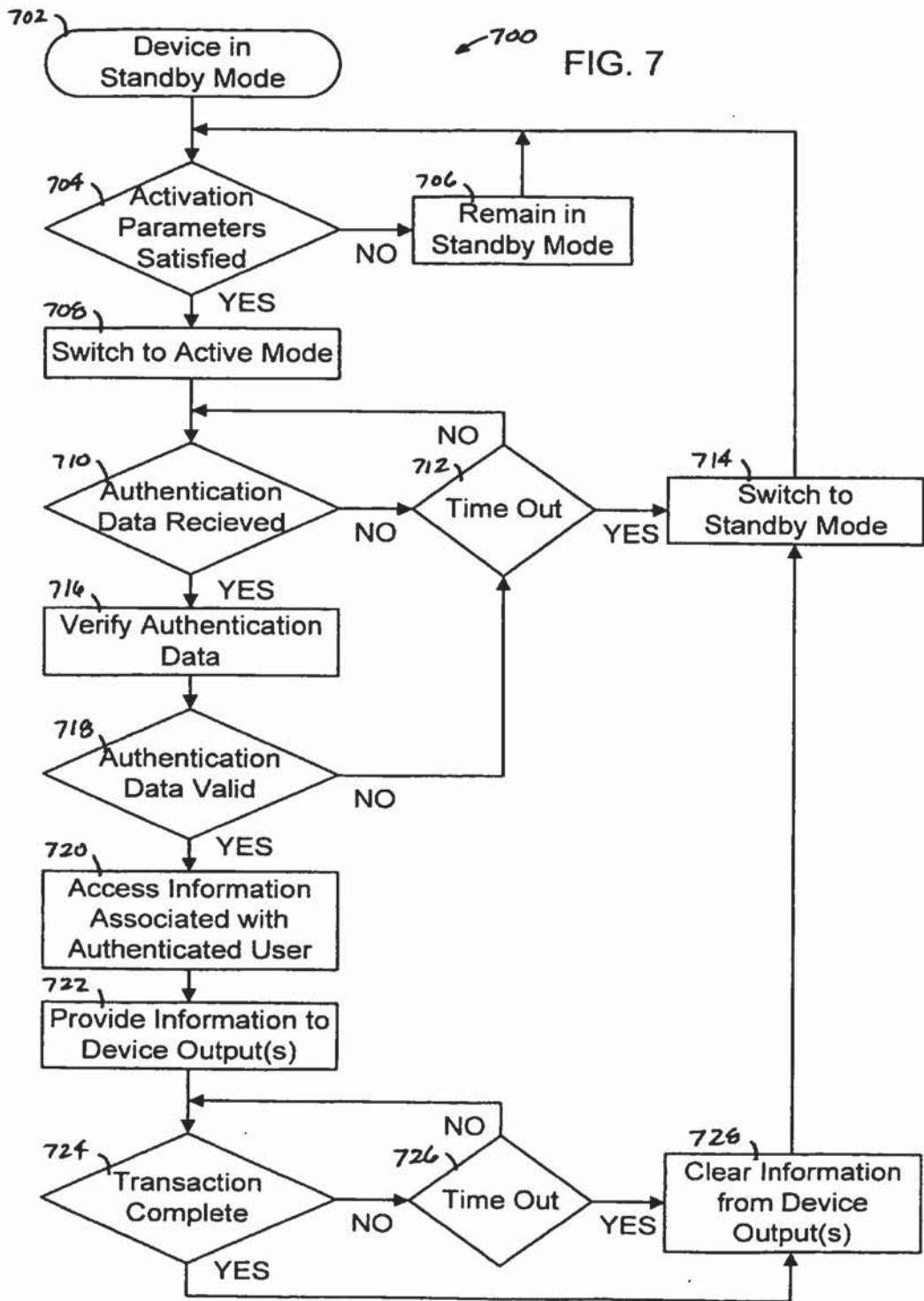


FIG. 6



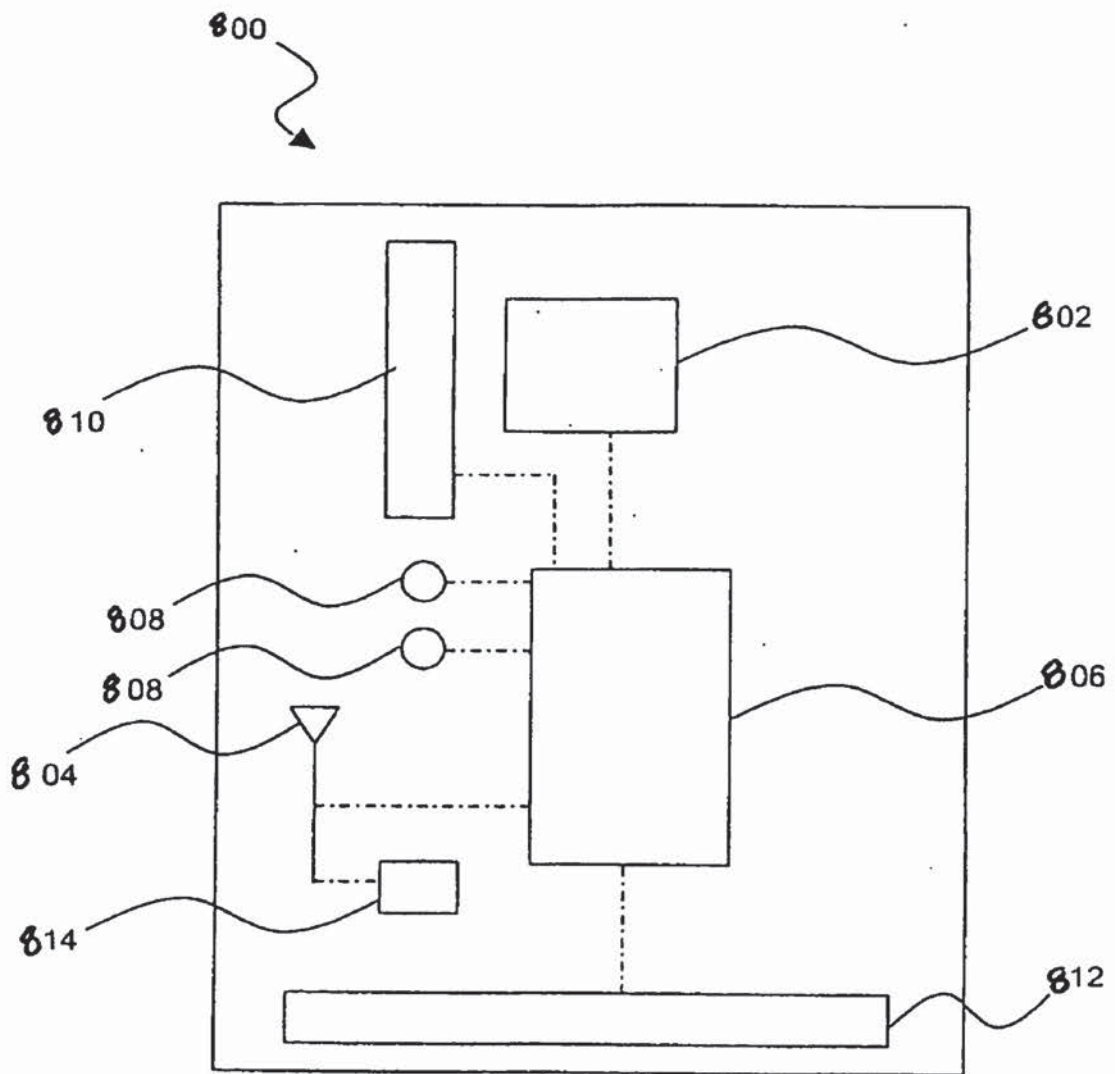


Fig. 8

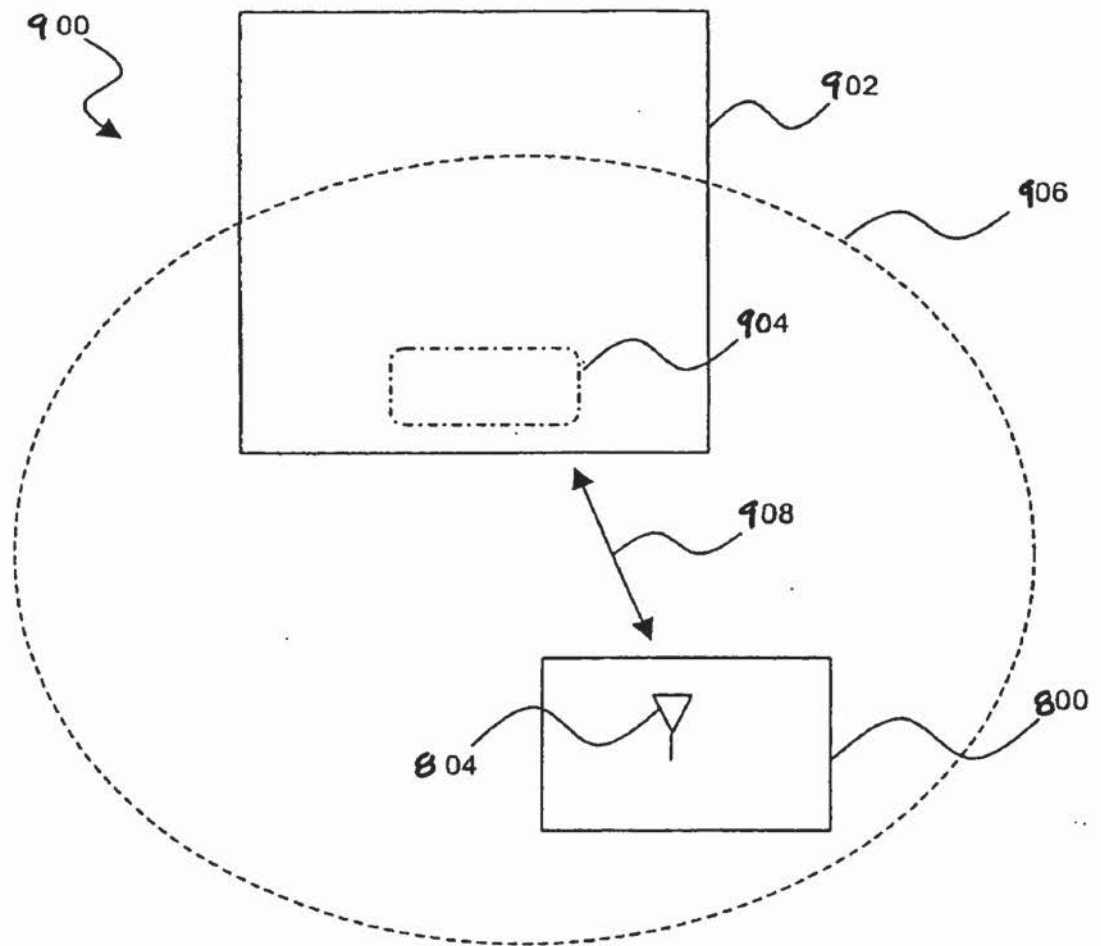


Fig. 9

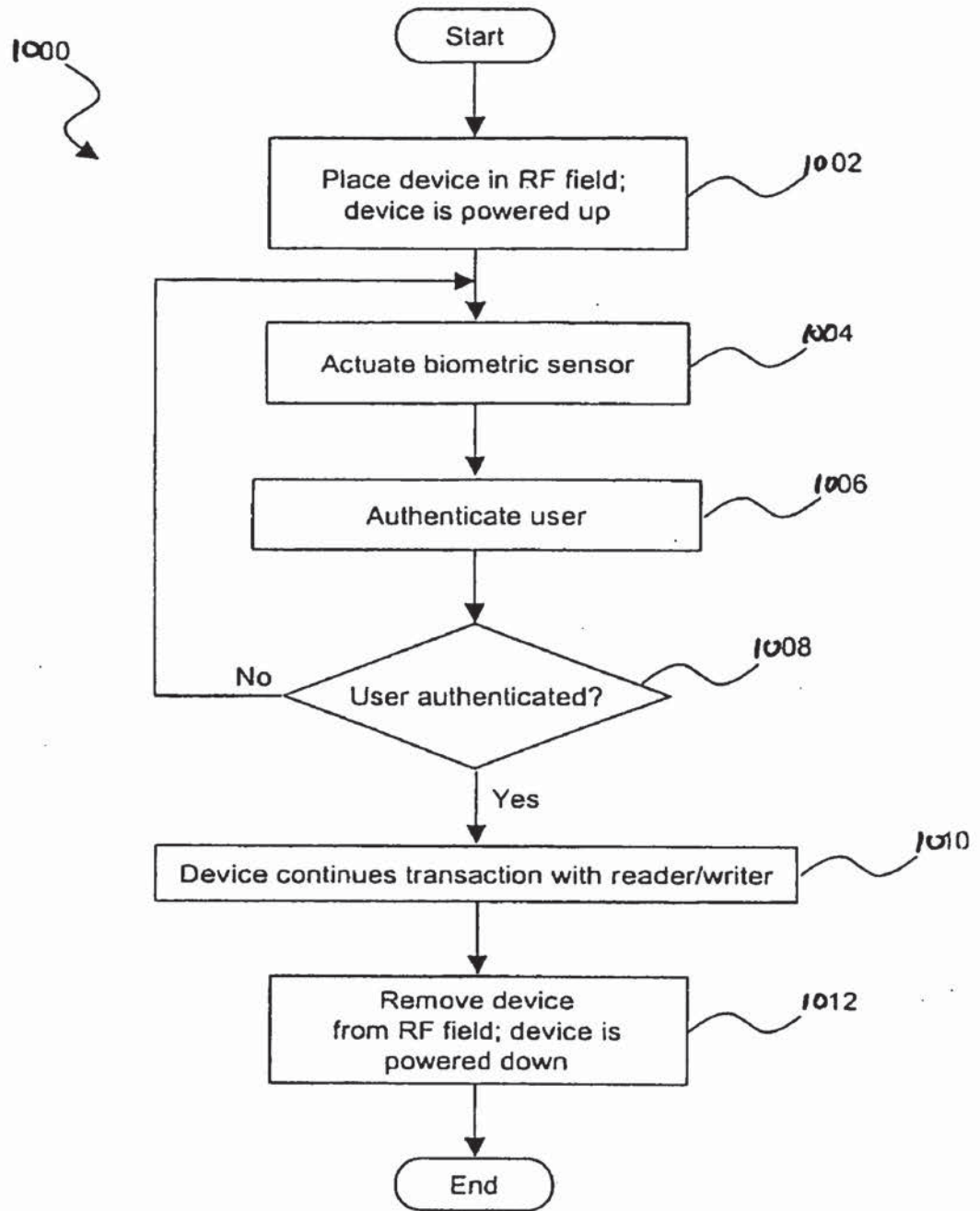


Fig. 10

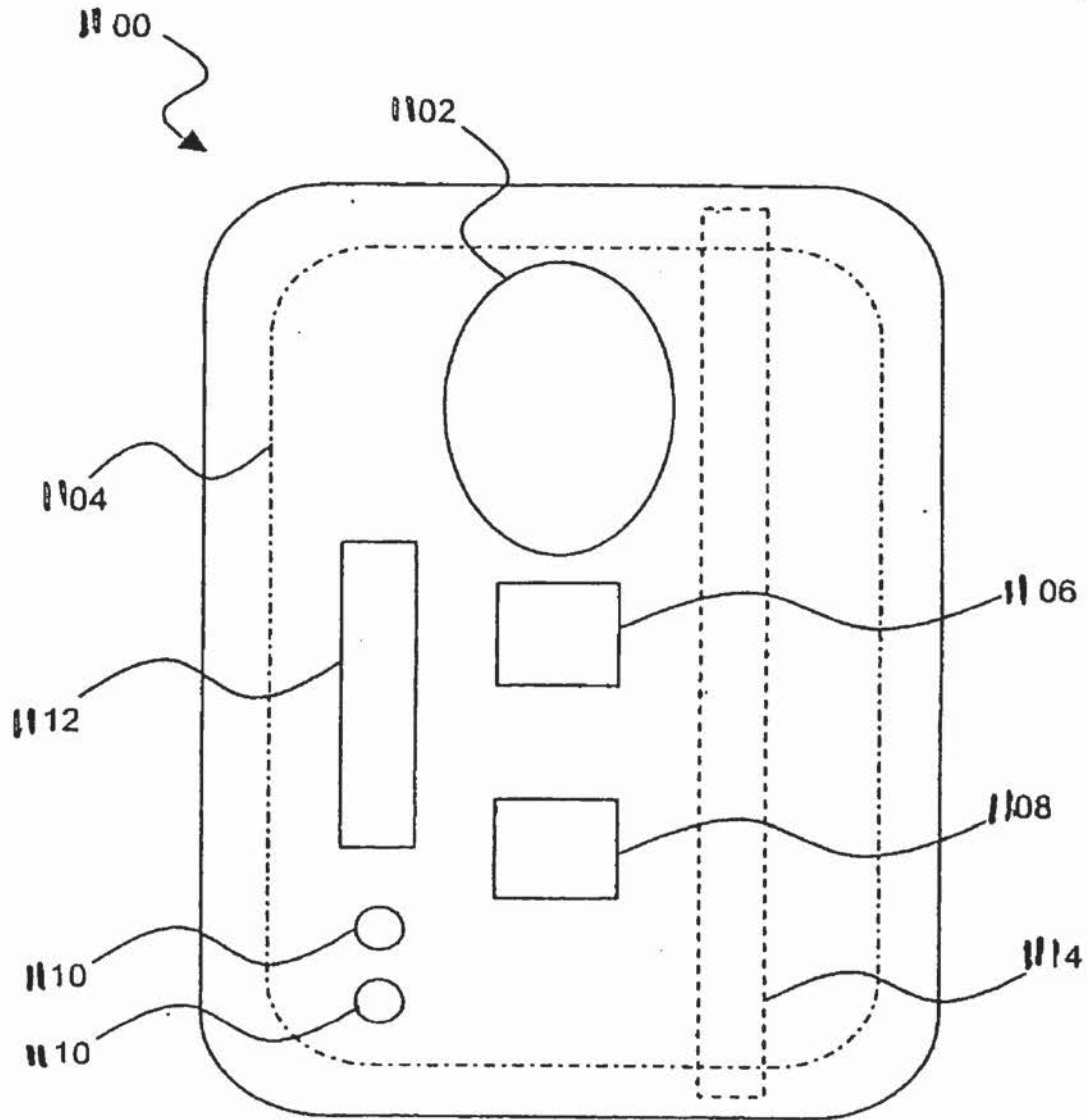


Fig. 11

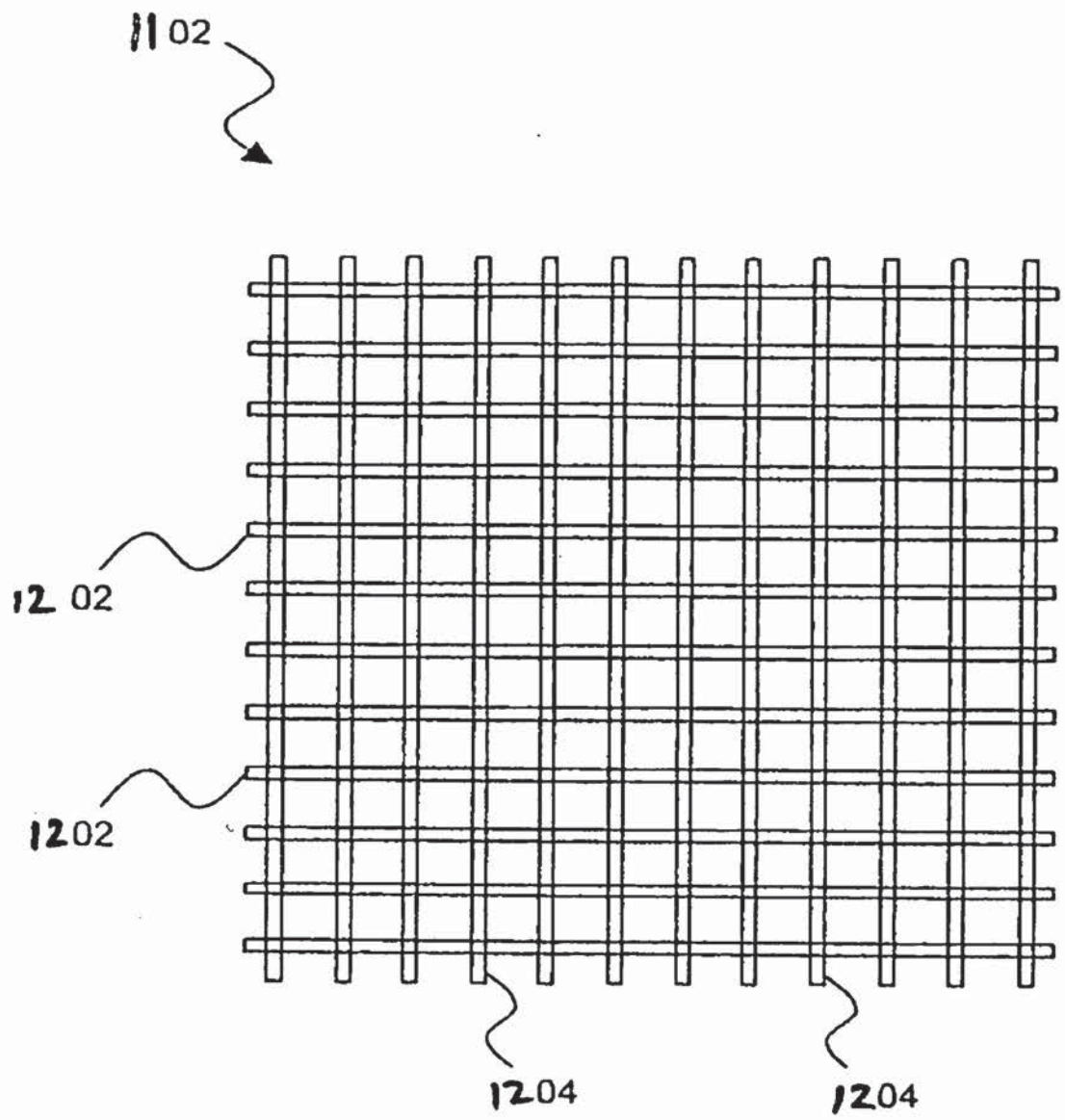


Fig. 12

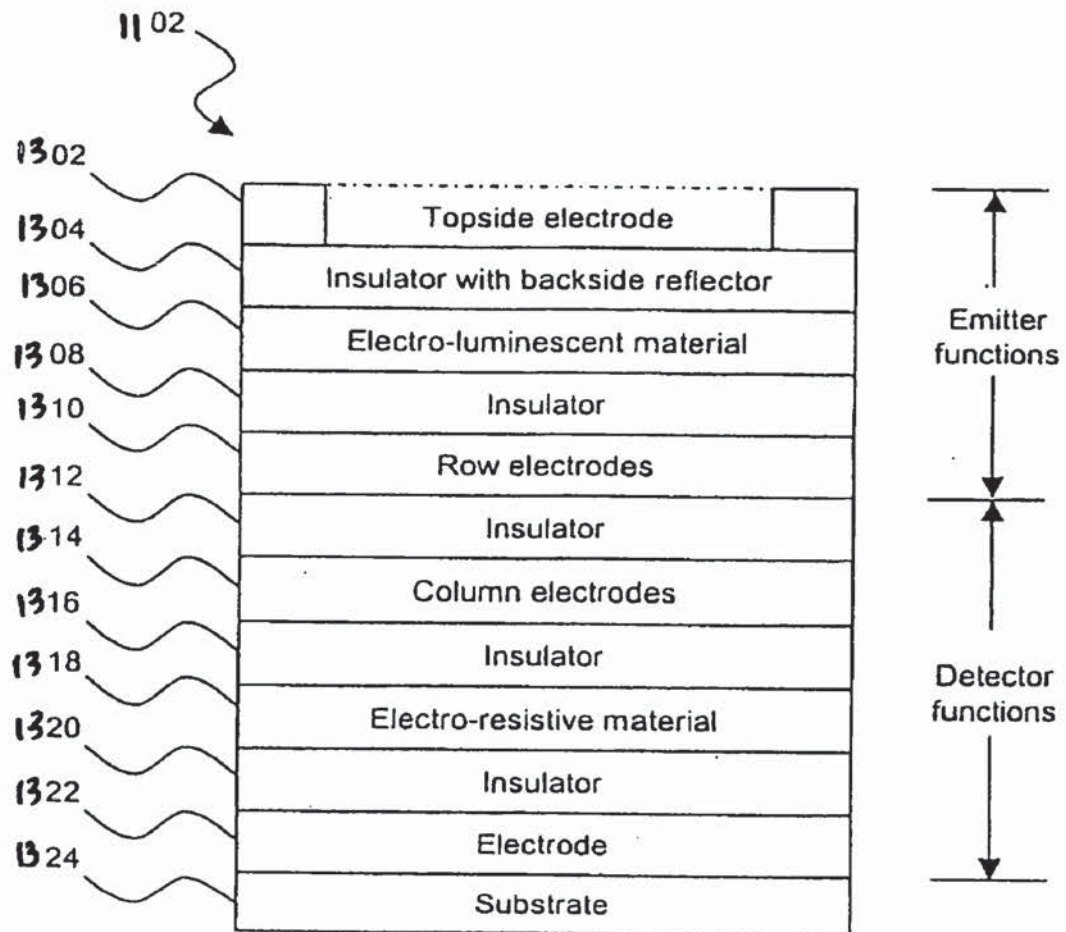


Fig. 13A

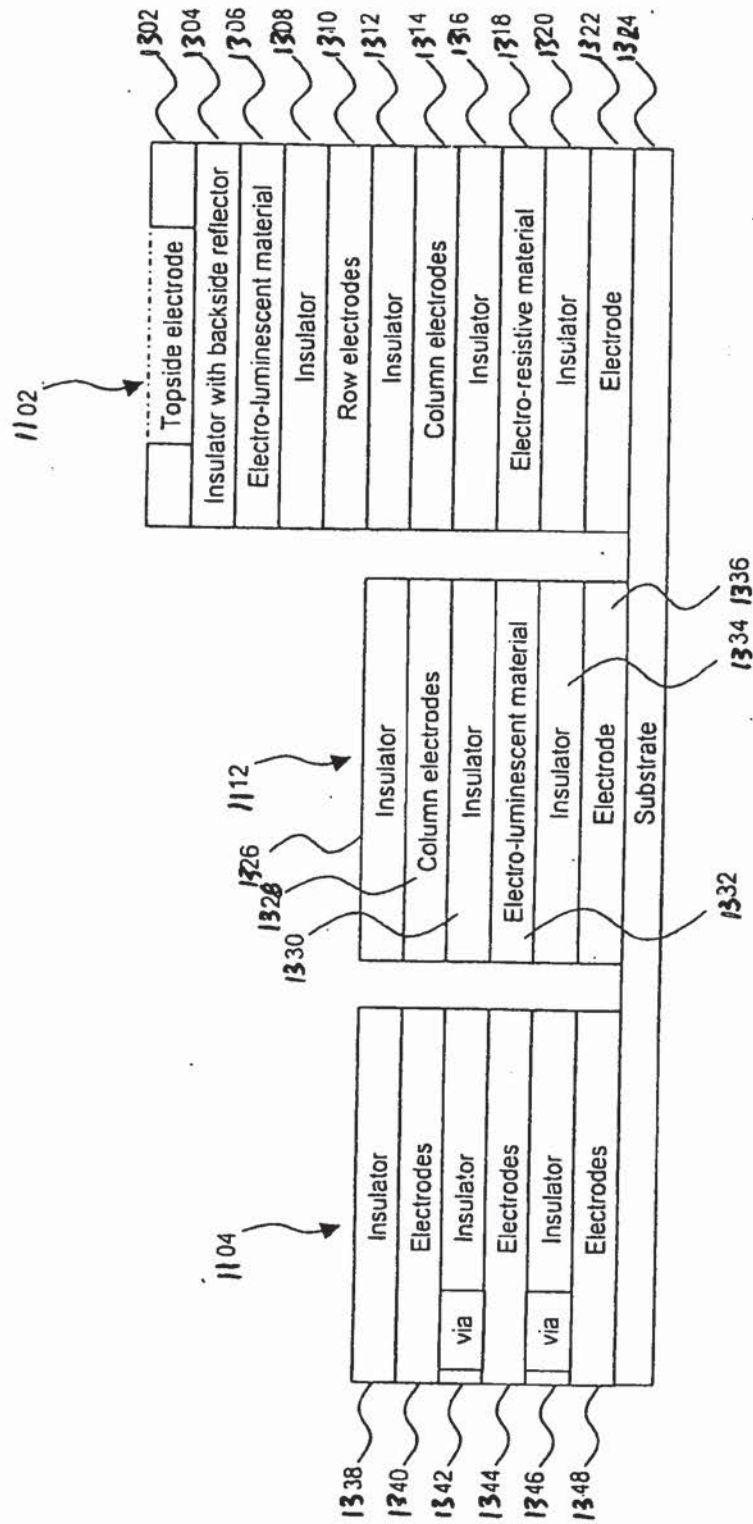


Fig. 13B

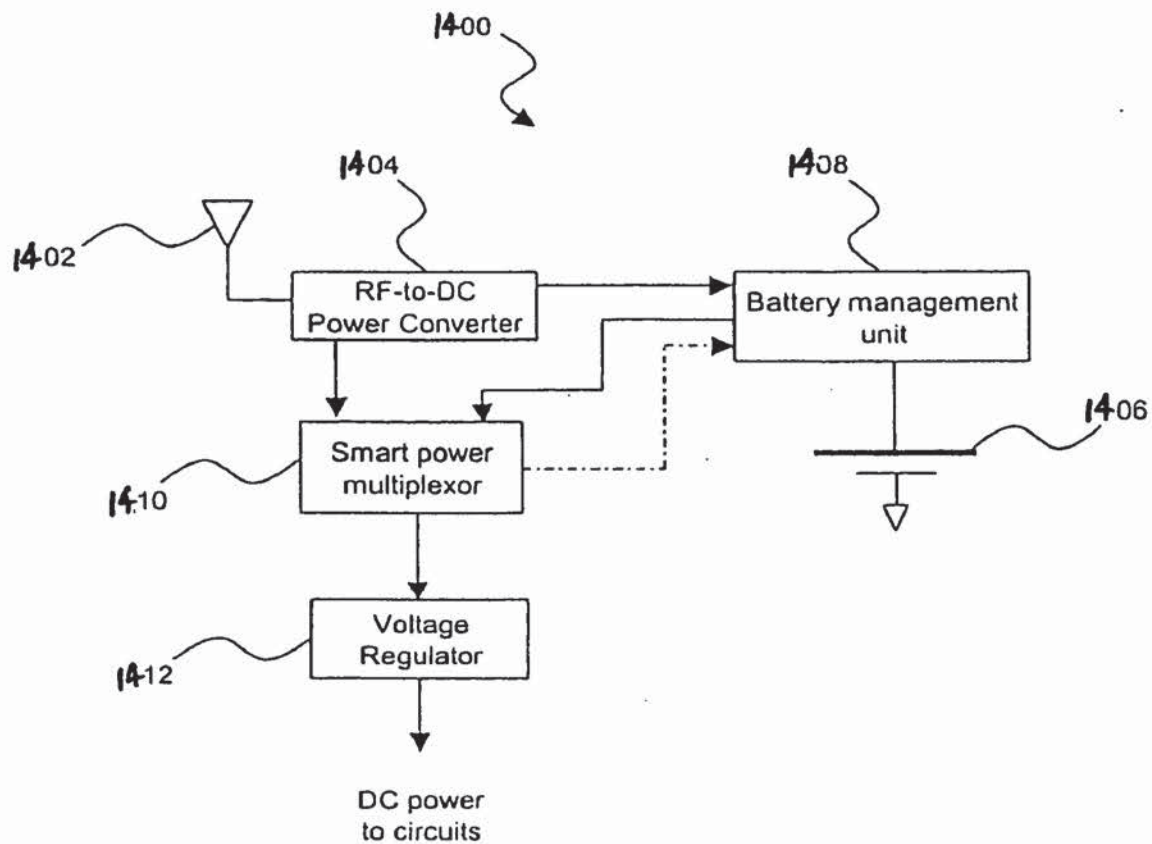


Fig. 14

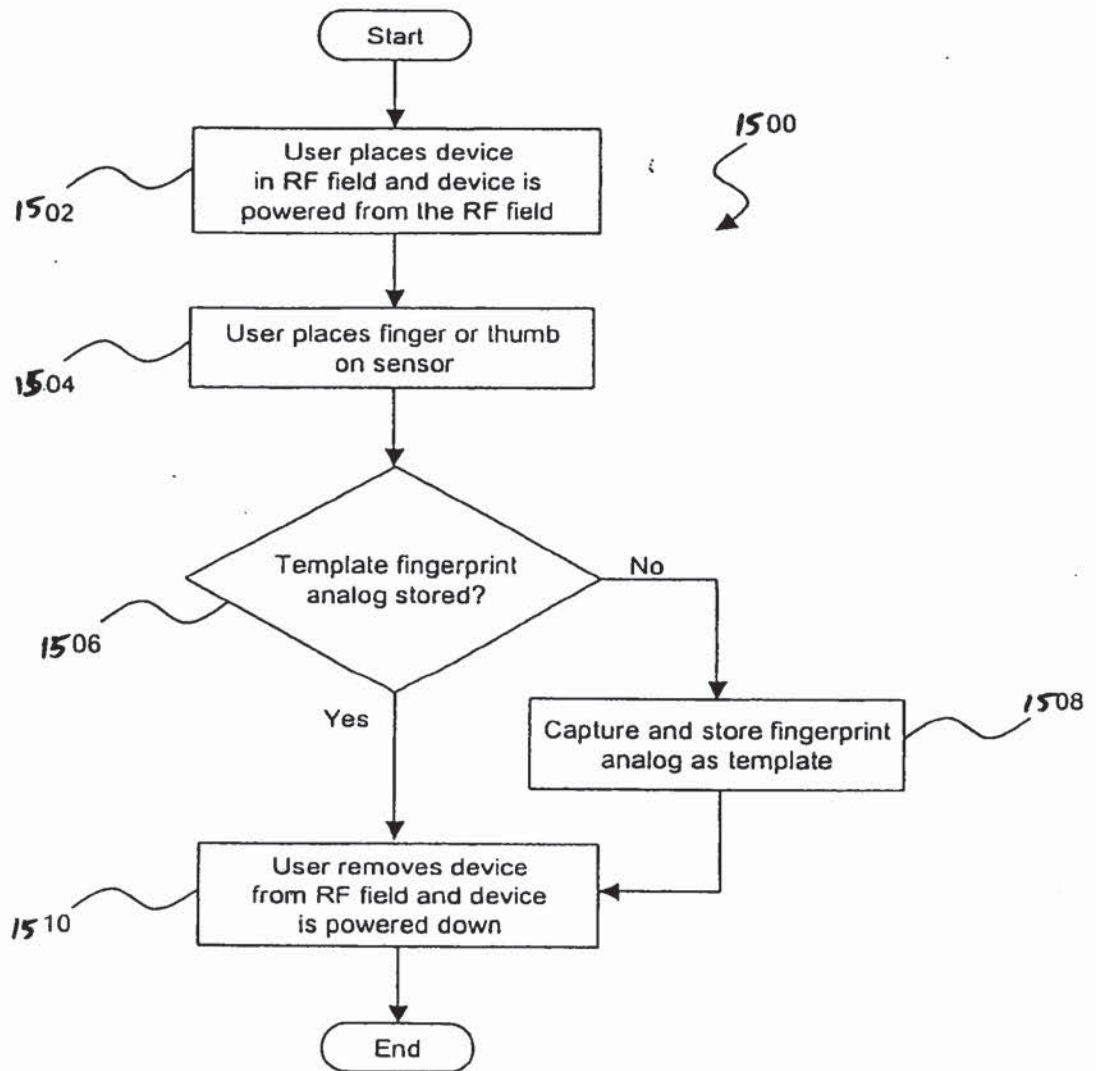


Fig. 15

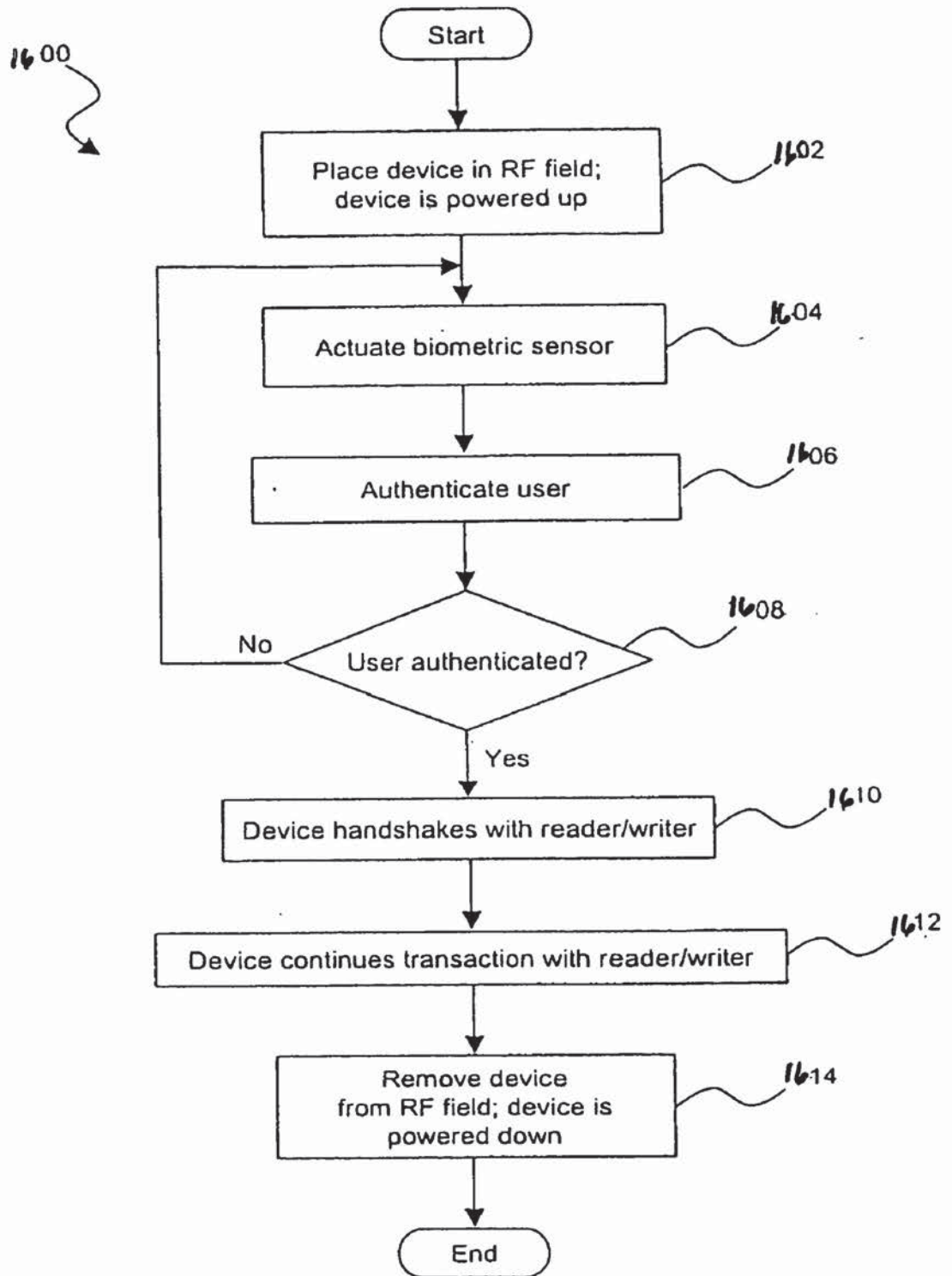


Fig. 16

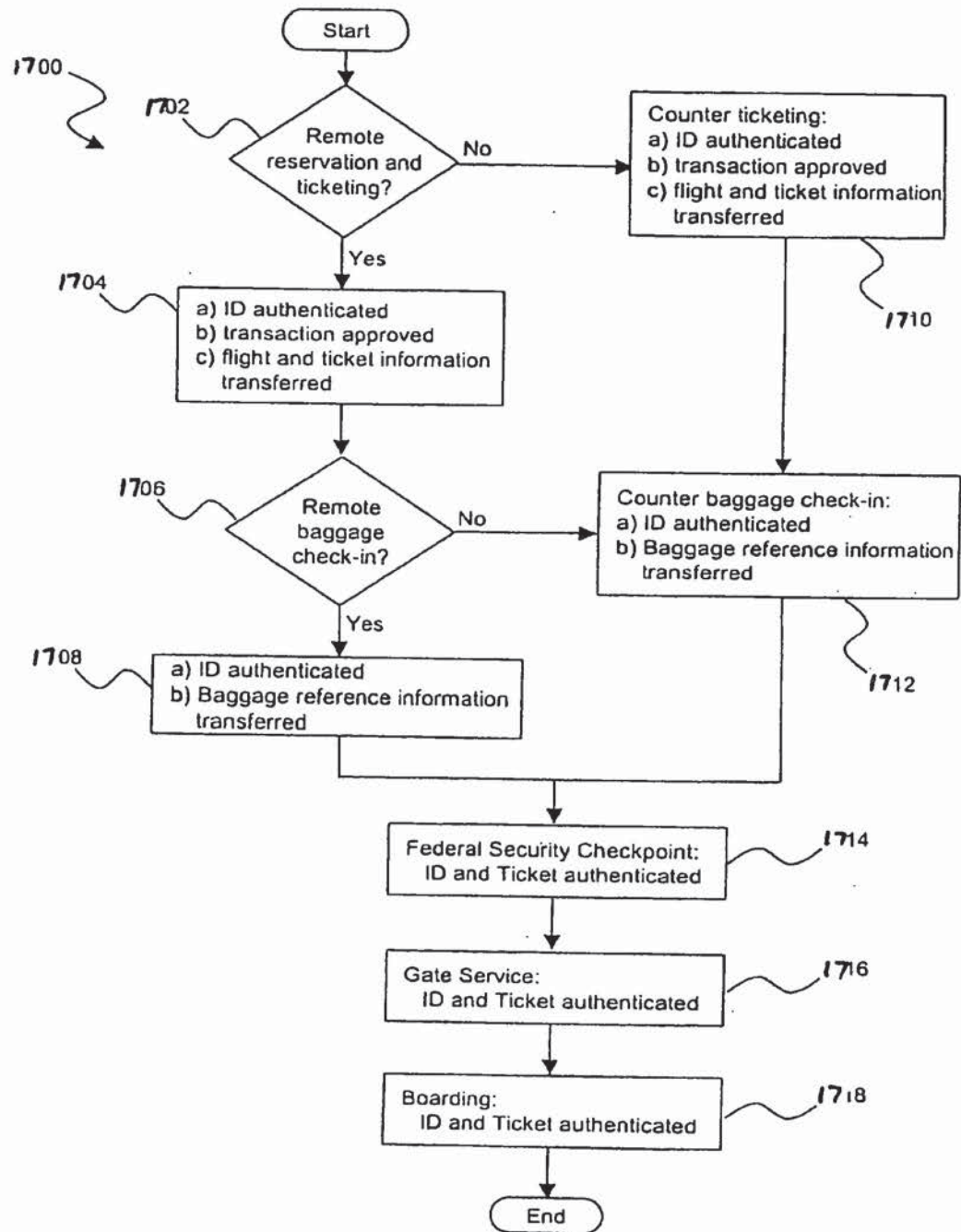


Fig. 17

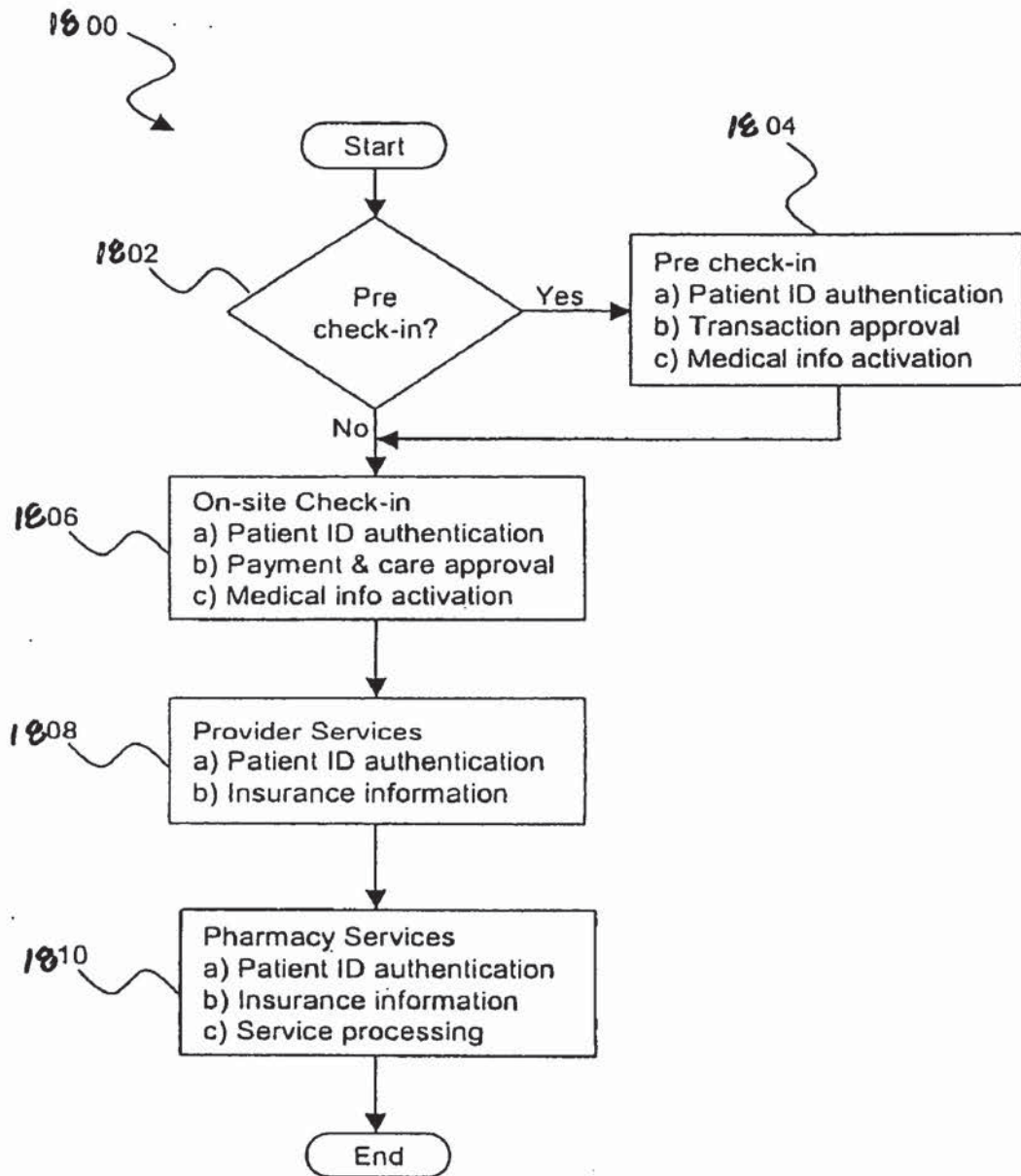


Fig. 18

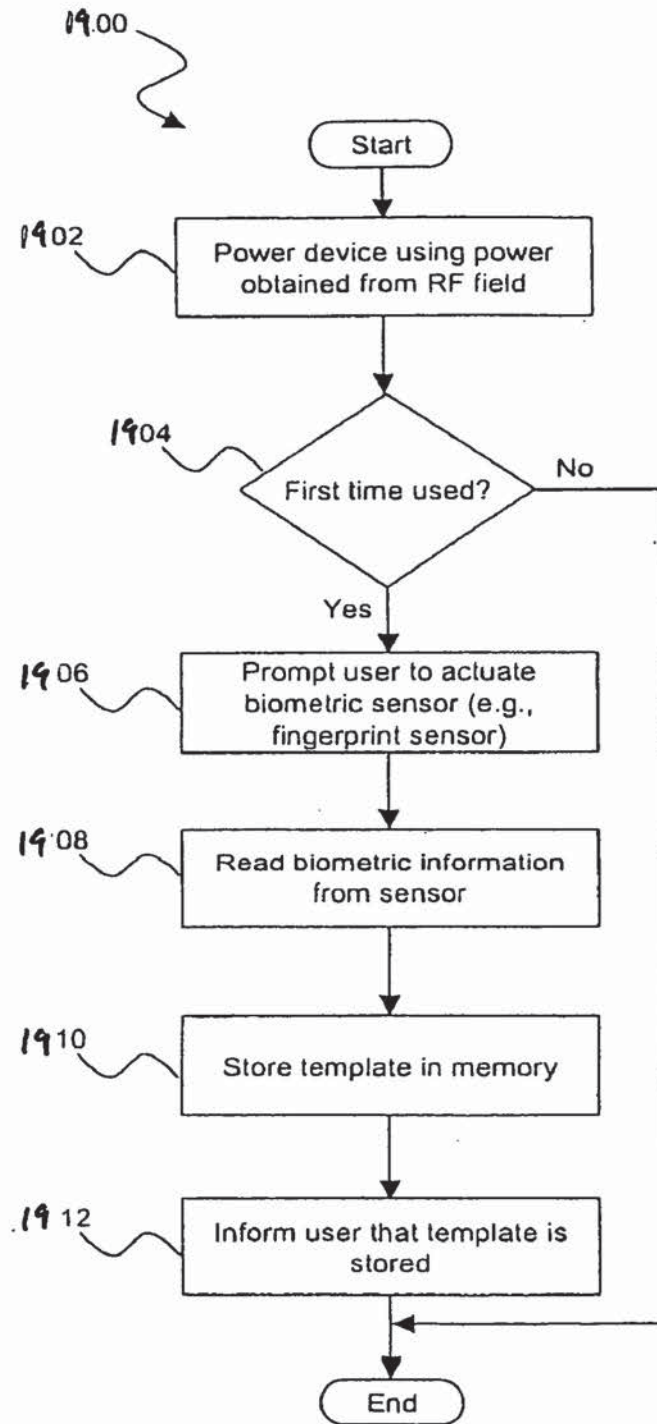


Fig. 19

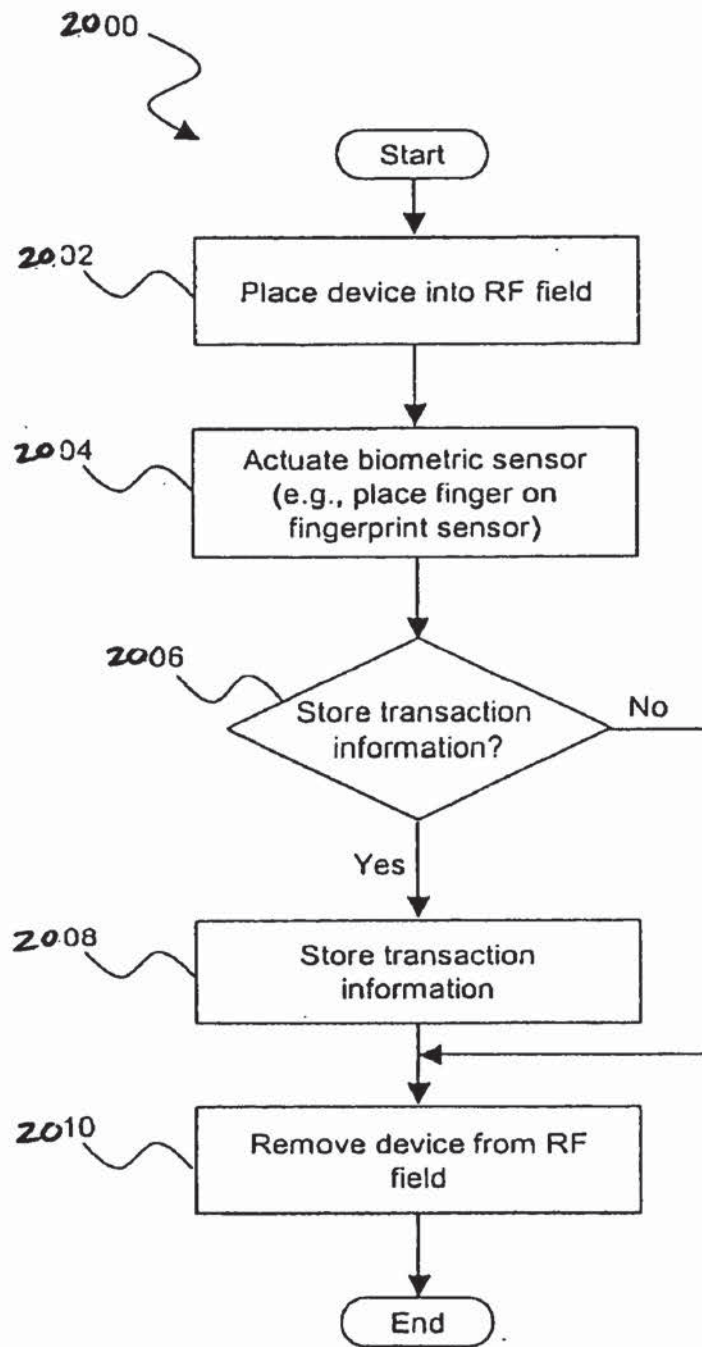


Fig. 20

**SYSTEM, METHOD AND APPARATUS FOR
ENABLING TRANSACTIONS USING A
BIOMETRICALLY ENABLED PROGRAMMABLE
MAGNETIC STRIPE**

PRIORITY CLAIM

[0001] This patent application is a continuation-in-part of U.S. patent application Ser. No. 10/400,306 filed on Mar. 27, 2003, which is a non-provisional patent application of U.S. provisional patent application serial No. 60/368,363 filed on Mar. 28, 2002.

TECHNICAL FIELD OF THE INVENTION

[0002] The present invention relates generally to the field of electronic devices and equipment used in the authentication and processing of commercial and security related transactions and, more particularly, to a system, method and apparatus for enabling transactions using biometrically enabled programmable magnetic stripes.

BACKGROUND OF THE INVENTION

[0003] The security of current magnetic stripe cards is suspect due to the ease of card theft and 'skimming' of card data for creating and using fake cards. As shown in FIG. 1, current magnetic stripe cards 100, such as access, credit, debit, identification, security, stored value and vendor-specific cards, typically have a strip of magnetic material 102, which is commonly referred to as a magnetic stripe, embedded in a plastic or laminated substrate 104. This magnetic stripe 102 carries data for the cardholder, such as name, account number, card expiration date, and other important information. This information is typically stored in three data tracks within the magnetic stripe 102 that carry a pattern of magnetization, which is a magnetic representation of the stored information. Other common features of magnetic stripe cards 100 that are well known to those skilled in the art, such as the cardholder's name, account number, expiration date, issuer, signature stripe, validation code, photograph, etc., are not shown. The magnetic patterns on the magnetic stripes 102 are easily created, read and damaged. As a result, the security of cards 100 that rely solely on magnetic stripes 102 for information storage and authentication is low and renders their use in applications involving highly sensitive information suspect. These types of cards are easily stolen and/or the data is "skimmed" for the creation and use of fake or counterfeit cards.

[0004] One way to increase the security of information bearing cards is the use of smart cards, also referred to as chip cards. Although smart cards 200 may also include a magnetic stripe, they primarily rely on an integrated circuit, also commonly referred to as a controller or processor, embedded within the plastic or laminated substrate 204 below the terminals 202 to store the cardholder's information as shown in FIG. 2. The integrated circuit is communicably coupled to a set of metallic terminals 202 that are designed to interface with a special reader. Other common features of smart cards 200 that are well known to those skilled in the art, such as the cardholder's name, account number, expiration date, issuer, signature stripe, validation code, photograph, etc., are not shown. A smart card 200 is capable of incorporating multiple applications or accounts on a single card or other media. As a result, smart cards 200

are widely recognized as a viable way to improve the effectiveness and security of a given card or device. Such smart cards 200 require a different reader from the standard magnetic stripe readers that currently make up virtually the entire card reader infrastructure throughout the world. As a result, the acceptance and wide-spread use of "true" smart cards (without a magnetic stripe) has been slow.

[0005] Various compromise technologies have been developed that incorporate some of the flexibility and security features of smart cards into a magnetic stripe card using either an adapter or a programmable magnetic stripe. For example, a smart card to magnetic stripe adapter is disclosed in US Patent Application Publication 2003/0057278 A1 published on Mar. 27, 2003 entitled "Advanced Magnetic Stripe Bridge (AMSB)" by Jacob Y. Wong. The Wong patent application describes an adapter or bridge that is used with magnetic stripe card readers such that a smart card or other card without a magnetic stripe can be placed into the bridge and electrically connected to the card. The bridge has one edge that is the size of a credit card so that the bridge can be swiped through the magnetic stripe reader while the card is still in the bridge. With this link in place, the data from the card is transmitted from the on-card processor through the bridge in a format that emulates the data generated by swiping the track(s) of a typical magnetic card through a magnetic stripe reader. As a result, the magnetic stripe reader is able to accept data from the magnetic stripe-less card. Similarly, one developer, VIVOTech, Inc., places a fixed bridge in the magnetic stripe reader that is capable of receiving radio frequency ("RF") data and then emulates the feed of data into the magnetic stripe reader via RF to complete the transaction without requiring physical contact of the card with the reader. Both of these technologies require either a fixed or mobile adaptor to be added to the card-reader infrastructure to enable data to be read from the card. While this is possible, it is still a modification to the world-wide infrastructure that is undesirable for unfettered use of the card. The use of such a bridge is cumbersome, adds cost and reduces reliability. In addition, this method also does not incorporate authentication of the user to provide protections against skimming or use by unauthorized individuals.

[0006] The use of a programmable magnetic stripe is disclosed in US Patent Application Publication 2002/0003169 A1 published on Jan. 10, 2002 entitled "Universal Credit Card Apparatus and Method" by J. Carl Cooper. The Cooper patent application describes a card in which a number of electrical coils are built into the card with one coil under each data bit on the magnetic stripe on the card so that each coil, when excited under the control of the on-card processor, creates a magnetic field that can magnetize the data bit in the magnetic track to be either a 0 or 1, thereby yielding a binary code that, when applied in accordance with the ISO standard for magnetic stripe cards, can be read by standard card readers. With this on-card capability in place, the processor can essentially "write" any data stored in the processor's memory to the on-card magnetic stripe. As with the adapter, the Cooper patent application does not provide any protections against card skimming or use by unauthorized persons. Moreover, because of the need for numerous individual coils (one beneath each data bit on the magnetic stripe), significant cost is incurred when adding these coils to the on-card design. The power requirements of such a card are also problematic.

[0007] There is, therefore, a need for a practical and secure card that has the advantages of a smart card and will interface with magnetic stripe readers without the use of adapters. Moreover, there is a need for a proper authentication in multiple account/application cards and devices to reduce the risk to the device holder in the event of loss or fraudulent capture of the data within the multiple accounts on the device.

SUMMARY OF THE INVENTION

[0008] The present invention provides a system, method and apparatus for a practical and secure card or device that has the advantages of a smart card and will interface with existing world-wide magnetic stripe readers without the use of adapters or bridges. Moreover, the present invention allows for proper authentication in multiple account/application cards and devices to reduce the risk to the device holder due to loss of the device or fraudulent capture of the data within the multiple accounts on the device. As a result, the present invention provides a secure and flexible system for security and/or commercial transactions using access, credit, debit, identification, security, stored value and vendor-specific cards and/or devices.

[0009] The present invention as described herein provides stringent protections for magnetic stripe cards and devices through the use of on-card/device biometric authentication of the user and programmable magnetic stripes such that the data within the tracks of the stripe can be spatially manipulated and managed by the logic within the processor/controller of the card or device. This allows magnetic stripe data to be modified or completely erased for protection of the cardholder, and then re-created on-demand by the programmable features built into the card or device. Alternatively, the data can be stored in the on-card processor/controller and then transmitted via time-varying signal to the card reader thereby emulating the swipe of a magnetic stripe through the magnetic card reader. In addition, the card or device can provide such information via a contactless communication system. These capabilities also enable multiple sets of data and applications to be incorporated onto a single card, device or media, thereby making it a universal card/device with numerous sets of data (e.g., accounts) and/or applications that can be temporarily downloaded onto the magnetic stripe from the memory of the on-card processor, used in the desired application, and then modified or erased. Finally, some or all of the above features can be disabled until the owner of the card enables them through use of an on-card biometrics sensor and logic that is pre-registered to the cardholder. As a result, maximum security is guaranteed since the card cannot be used if it is lost or stolen, and skimming can be virtually eliminated by prompt modification or erasure of the magnetic stripe data following the basic transaction authorized by the owner.

[0010] The present invention provides an apparatus or user device that includes a substrate, a magnetic field generator disposed within the substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate and a processor disposed within the substrate that is communicably coupled to the magnetic field generator, the biometric sensor and the memory. The processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic

field generator when the user is verified. A power source is also disposed within the substrate and electrically connected to the magnetic field generator, the biometric sensor and the processor. The magnetic field generator can create a spatial magnetic signal using a magnetic stripe and one or more induction coils, or create a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader. As a result, the magnetic field generator emulates a programmable magnetic stripe.

[0011] The present invention also provides a method for enabling a transaction using an apparatus containing information associated with one or more users, a magnetic field generator that is normally inactive and a biometric sensor. The method includes the steps of receiving authentication data from the biometric sensor, determining whether the authentication data is valid for one of the users, and activating the magnetic field generator and generating a magnetic signal corresponding to the information associated with the authenticated user whenever the authentication data is valid. The method can be performed by a computer program, such as middleware, embodied in a computer readable medium wherein each step is implemented as one or more code segments.

[0012] In addition, the present invention provides a system having one or more user devices, one or more system interfaces operable to communicate with the user device and a system processor communicably coupled to the one or more system interfaces. Each user device includes a substrate, a magnetic field generator disposed within the substrate that is normally inactive, a biometric sensor mounted on the substrate, a memory disposed within the substrate and a device processor disposed within the substrate and communicably coupled to the magnetic field generator, the biometric sensor and the memory. The device processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified. The user device also includes a power source disposed within the substrate and electrically connected to the magnetic field generator, the biometric sensor and the device processor.

BRIEF DESCRIPTION OF THE DRAWINGS

[0013] For a more complete understanding of the features and advantages of the present invention, reference is now made to the detailed description of the invention along with the accompanying figures in which corresponding numerals in the different figures refer to corresponding parts and in which:

[0014] FIG. 1 depicts a standard credit card with a magnetic stripe in accordance with the prior art;

[0015] FIG. 2 depicts a smart card in accordance with the prior art;

[0016] FIG. 3 depicts a block diagram of a system for enabling transactions in accordance with one embodiment of the present invention;

[0017] FIG. 4A depicts the front of an exemplary embodiment of a card for enabling transactions using a biometrically enabled programmable magnetic stripe in accordance with the present invention;

[0018] FIG. 4B depict the back of an exemplary embodiment of a card for enabling transactions using a biometrically enabled programmable magnetic stripe in accordance with the present invention;

[0019] FIG. 5A depicts a block diagram of a programmable magnetic stripe using multiple inductive coils in accordance with one embodiment of the present invention;

[0020] FIG. 5B depicts a block diagram of a programmable magnetic stripe using a single induction coil for sending emulated time-varying magnetic stripe data to a magnetic card reader directly from the on-card controller in accordance with another embodiment of the present invention;

[0021] FIG. 6 depicts an exemplary embodiment of the combined elements of a biometrically enabled programmable magnetic stripe on a device for secure physical and commercial transactions in accordance with the present invention;

[0022] FIG. 7 is a flow chart of an exemplary authentication method for using a device in accordance with the present invention;

[0023] FIG. 8 depicts one embodiment of an exemplary device for effecting secure physical and commercial transactions in a contactless manner using biometrics identity validation in accordance with the present invention;

[0024] FIG. 9 depicts an exemplary environment in which the device of FIG. 8 may operate in accordance with the present invention;

[0025] FIG. 10 is a flow chart of an exemplary method for using the device of FIG. 8 in the environment of FIG. 9 in accordance with the present invention;

[0026] FIG. 11 is a diagram illustrating another embodiment of an exemplary device for effecting secure physical and commercial transactions in a contactless manner using biometrics identity validation in accordance with the present invention;

[0027] FIG. 12 is an illustration of one embodiment of a biometric sensor that may be used in the device of FIG. 11 in accordance with the present invention;

[0028] FIG. 13A illustrates various layers that form one embodiment of the biometric sensor of FIG. 12 in accordance with the present invention;

[0029] FIG. 13B illustrates various layers that form a portion of one embodiment of the device of FIG. 11 in accordance with the present invention;

[0030] FIG. 14 is a diagram of an exemplary power circuit that may be used in the device of FIG. 11 in accordance with the present invention;

[0031] FIG. 15 is a flow chart of an exemplary method for storing a template fingerprint analog in the device of FIG. 11 in accordance with the present invention;

[0032] FIG. 16 is a flow chart of an exemplary method for using the device of FIG. 11 in accordance with the present invention;

[0033] FIG. 17 is a flow chart of an exemplary method for using the device of FIG. 1 in an air transportation environment in accordance with the present invention;

[0034] FIG. 18 is a flow chart of an exemplary method for using the device of FIG. 1 in a healthcare environment in accordance with the present invention;

[0035] FIG. 19 is flow chart of an exemplary method for storing a biometric template analog in the device of FIG. 8 in accordance with the present invention; and

[0036] FIG. 20 is a flow chart of an exemplary method for using the device of FIG. 8 in a financial transaction in accordance with the present invention.

DETAILED DESCRIPTION OF ILLUSTRATIVE EMBODIMENTS

[0037] While the production and application of various embodiments of the present invention are discussed in detail below in relation to authentication and processing of commercial and security related transactions, it should be appreciated that the present invention provides many applicable inventive concepts that may be embodied in a wide variety of specific contexts. The specific embodiments discussed herein are merely illustrative of specific ways to make and use the invention and do not delimit the scope of the invention.

[0038] The present invention provides a system, method and apparatus for a practical and secure card or device that has the advantages of a smart card and will interface with existing world-wide magnetic stripe readers without the use of adapters or bridges. Moreover, the present invention allows for proper authentication in multiple account/application cards and devices to reduce the risk to the device holder due to loss of the device or fraudulent capture of the data within the multiple accounts on the device. As a result, the present invention provides a secure and flexible system for security and/or commercial transactions using access, credit, debit, identification, security, stored value and vendor-specific cards and/or devices.

[0039] The present invention as described herein provides stringent protections for magnetic stripe cards and devices through the use of on-card/device biometric authentication of the user and programmable magnetic stripes such that the data within the tracks of the stripe can be manipulated and managed by the logic within the processor/controller of the card or device. This allows magnetic stripe data to be modified or completely erased for protection of the cardholder, and then re-created on-demand by the programmable features built into the card or device. Alternatively, the data can be stored in the on-card processor/controller and then transmitted via time-varying signal to the card reader thereby emulating the swipe of a magnetic stripe through the magnetic card reader. In addition, the card or device can provide such information via a contactless communication system. These capabilities also enable multiple sets of data and applications to be incorporated onto a single card, device or media, thereby making it a universal card/device with numerous sets of data (e.g., accounts) and/or applications that can be temporarily downloaded onto the magnetic stripe from the memory of the on-card processor, used in the desired application, and then modified or erased. Finally, some or all of the above features can be disabled until the owner of the card enables them through use of an on-card biometrics sensor and logic that is pre-registered to the cardholder. As a result, maximum security is guaranteed since the card cannot be used if it is lost or stolen, and

skimming can be virtually eliminated by prompt modification or erasure of the magnetic stripe data following the basic transaction authorized by the owner.

[0040] Now referring to FIG. 3, a block diagram of a system 300 for enabling transactions in accordance with one embodiment of the present invention is shown. More specifically, the present invention provides a system 300 having one or more user devices 302, one or more system interfaces 304 operable to communicate with the user device(s) 302 and a system processor or controller 306 communicably coupled to the one or more system interfaces 304. Each user device 302 includes a magnetic field generator 308 that is normally inactive, a biometric sensor 310, a memory 312, a device processor or controller 314 and a power source 316. Note that the memory 312 and device processor 314 may be integrated into a single integrated circuit. The device processor 314 may also include a smart card processor and an application specific integrated circuit ("ASIC") chip. In addition, the power source 316 may be controlled by a power management unit 318. The magnetic field generator 308, biometric sensor 310 and memory 312 are all communicably coupled to the device processor 314. The magnetic field generator 308, biometric sensor 310, memory 312 and device processor 314 are all electrically connected to the power source 316 via the power management unit 318. If the user device 302 does not include a power management unit 318, the magnetic field generator 308, biometric sensor 310, memory 312 and device processor 314 will all be electrically connected to the power source 316. The device processor 314 is operable to process biometric information received from the biometric sensor 310 to verify that a user is authorized to use the device 302 and activate the magnetic field generator 308 when the user is verified.

[0041] The magnetic field generator 308 emulates a programmable magnetic stripe by either creating a spatial magnetic signal or a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader (See FIG. 5B). The spatial magnetic signal is created using a magnetic stripe either mounted on the substrate or disposed within the substrate, one or more induction coils disposed within the substrate underneath the magnetic stripe, and a controller disposed within the substrate that is connected to the one or more induction coils and operable to generate a magnetic signal via the one or more induction coils and the magnetic stripe (See FIG. 5B). In either case, the magnetic signal includes binary data to enable a transaction, such as a user name, user number, device expiration date, transaction approval/denial, etc. A typical magnetic stripe contains three-tracks wherein each track contains a set of magnetic data cells. Note that the magnetic field generator 308 may be configured to read a magnetic stripe from another device so that device 302 can replace the other device. The information read from the magnetic stripe would be stored in memory 312 for later transmission by the magnetic field generator 308 upon proper authentication.

[0042] The biometric sensor 310 may include a fingerprint sensor, retina sensor or voice sensor or other sensor device capable of detecting unique characteristics of a person that can then be compared to stored data. One example of such a fingerprint sensor includes a matrix of points operable to detect high and low points corresponding to ridges and valleys of a fingerprint. Another example of a fingerprint

sensor includes an emitter and a detector wherein light projected by the emitter is reflected from a user's finger onto the detector.

[0043] When the device 302 is initialized or linked to a user, the biometric sensor 310 is used to collect biometric information about the user. This biometric information is stored as a biometric analog of the user in the memory 312. Thereafter, and as will be described below in reference to FIG. 7, biometric information or authentication data is obtained by the biometric sensor 310 and sent to the device processor 314 for authentication. The device processor 314 determines whether the authentication data is valid for one of the users by comparing the authentication data to the biometric template stored in memory 312. If the authentication data is valid, the device processor 314 activates the magnetic field generator 308 and provides binary data to the magnetic field generator 308 to be transmitted as a magnetic signal. The magnetic field generator 308 then generates the magnetic signal corresponding to the information associated with the authenticated user and the selected application. The device processor 314 will then deactivate the magnetic field generator 308 after the magnetic field generator 308 has been active for a specified period of time. Alternatively, the device processor 314 may deactivate the magnetic field generator 308 when the biometric sensor 310 no longer detects the authorized user, or a transaction complete signal is received. The present invention reduces power consumption of the device 302 and increases security by (1) keeping the magnetic field generator 308 normally inactive, (2) activating the magnetic field generator 308 and transmitting the magnetic signal only after the user has been authenticated, and (3) disabling the magnetic field generator sometime thereafter. Additional power consumption can be reduced by keeping the device 302 in a sleep or low power mode until certain activation parameters have been satisfied, such as receiving an external signal, contact with the biometric sensor 310 or a user input/command.

[0044] The power source 316 may include a battery, a piezoelectric generator, a solar panel, an electromagnetic energy converter (such as used in passive Radio Frequency Identification ("RFID") systems), a kinetic energy converter or any combination thereof. For example, the power source 316 may include a battery, a power generator, a converter and a multiplexer. The converter is electrically connected to the power generator and operable to convert power received from the power generator into power usable by the device 302 or to charge the battery. The battery management unit 318 is connected to the battery. The power multiplexer is connected to the battery management unit 318 and the converter. The power multiplexer is operable to determine whether to draw power from the battery management unit, from the converter, or from both.

[0045] The device 302 may also include a user interface 320 that is communicably coupled to the device processor 314 and electrically connected to the power source 316 (via power management unit 318). The user interface 320 may include a touch pad, one or more buttons, a display, a voice sensor or other known user interfaces. The device 302 may also include a contactless interface 322 that is communicably coupled to the device processor 314 and electrically connected to the power source 316 (via power management unit 318). The contactless interface 322 may include an antenna for wireless communication, an optical transceiver

or other known contactless communication methods. In addition, device 302 may also include a smart card interface 324 that is communicably coupled to the device processor 314 and electrically connected to the power source 316 (via power management unit 318). Moreover, device 302 may include an optical or other type of input/output (VO) interface 326 that is communicably coupled to the device processor 314 and electrically connected to the power source 316 (via power management unit 318).

[0046] The components of the device 302 are typically disposed within or mounted on a substrate. For example, the biometric sensor 310, user interface 320, smart card interface 324 and optical or other I/O interface 326 are typically mounted on the substrate; whereas the memory 312, device processor 314, power source 316 and power management unit 318 are typically disposed within the substrate. The magnetic field generator 308 and contactless interface 322 can be mounted on the substrate or disposed within the substrate. The type of material used for the substrate and the resulting properties of the substrate will depend on the desired application and working environment for the device 302. In many cases, the substrate will be a semi-flexible material, such as plastic, or a laminate material. The substrate can then be integrated into a card, such as an access card, a credit card, a debit card, an identification card, a mini-card, a security card, a stored value card and a vendor-specific card, etc. The substrate may also be integrated into a travel credential, such as a passport, an immigration card and a visa, etc. In addition, the substrate may be integrated into a personal communication device, such as a personal data assistant (PDA), a telecommunications device, a pager, a computer and an electronic mail transceiver, etc. Moreover, the substrate may be integrated into a personal device/belonging, such as a watch, a jewelry, a key ring, a tag and eye glasses, etc.

[0047] The one or more system interfaces 304 may include a device initialization interface 328, a magnetic reader 330, a wireless communications interface (transceiver) 332, a smart card reader 334, or an optical or other input/output interface 336. The one or more system interfaces 304 are used to communicate with the user device 302 physically or contactlessly, depending on the desired application and implementation. Other non-system interfaces may include a battery recharger, personal computer interface or personal data assistant (PDA). The one or more system interfaces 304 are communicably coupled to a system processor or controller 306, which in turn may be communicably coupled to a database 338 or one or more remote systems or computers 342 via network 340. Network 340 may be a local area network or wide area network, such as the Internet.

[0048] Referring now to FIG. 4A, the front 400 of an exemplary embodiment of a card for enabling transactions using a biometrically enabled programmable magnetic stripe in accordance with the present invention is shown. The card is shown in the form of a credit or debit card, but may also be used as an access card, an identification card, a mini-card, a security card, a stored value card and a vendor-specific card, etc. The front 400 of the card includes the issuer's name 402, a biometric sensor 310, a photo or I/O interface 404 (user interface 320 or other I/O interface 326), a smart card interface 324, a card number 406, an expiration date 408, the card holder's name 410 and a hologram 412. Other information and features may also be placed on or within the

card. As will be appreciated by those skilled in the art, the features described above can be rearranged or eliminated to fit a specific application for the card.

[0049] Now referring to FIG. 4B, the back 450 of an exemplary embodiment of a card for enabling transactions using a biometrically enabled programmable magnetic stripe in accordance with the present invention is shown. The back 450 of the card includes the magnetic field generator 308 (programmable magnetic stripe), an area for the card holder to place an authorized signature 452 and the issuer's contact information and disclaimers 454. Other information and features may also be placed on or within the card. As will be appreciated by those skilled in the art, the features described above can be rearranged or eliminated to fit a specific application for the card.

[0050] Referring now to FIG. 5A, a block diagram of a programmable magnetic stripe 500 (308FIG. 3) using multiple inductive coils 518-530 in accordance with one embodiment of the present invention is shown. The programmable magnetic stripe 500 (308FIG. 3) includes a magnetic stripe 502, multiple inductive coils 518-530 and a control circuit 532. The magnetic stripe 502 contains one or more sets of magnetic data cells 504-516. For example, magnetic stripe 502 will typically contain three tracks or sets of magnetic data cells 504-516. The individual inductive coils 518-530 are mounted immediately beneath each of the binary magnetic data cells 504-516. Each inductive coil 518-530 is electrically connected to the control circuit 532, which may be integrated into the device processor 314 (FIG. 3). When a positive or negative current is applied to each inductive coil 518-530, it changes the polarity of the magnetized particles in the binary magnetic data cell 504-516 of the data track in the magnetic stripe 502 immediately above it, thereby creating a spatially varying binary code or magnetic signal in the magnetic stripe 502 material that can be read by standard magnetic card readers when such binary code is applied in accordance with ISO standards.

[0051] Now referring to FIG. 5B, a block diagram of a programmable magnetic stripe 550 (308FIG. 3) using a single induction coil 552 for sending emulated time-varying magnetic stripe data to a magnetic card reader directly from the on-card controller in accordance with another embodiment of the present invention is shown. The programmable magnetic stripe 550 (308FIG. 3) includes a magnetic stripe 502, a single inductive coil 552 and a control circuit 554. The magnetic stripe 502 contains one or more sets of magnetic data cells 504-516. For example, magnetic stripe 502 will typically contain three tracks or sets of magnetic data cells 504-516. The long inductive coil 552 is mounted immediately beneath the entire length of the magnetic stripe 502 and its corresponding binary magnetic data cells 504-516 such that a time-varying signal can be transmitted to the heads of the magnetic card reader as the card is swiped through the reader. The data rate is determined based on the minimum and maximum swipe speeds that standard readers can accommodate. In other words, the single inductive coil 552 is long enough for it to be in the physical proximity of the card reader heads for the entire time period required to transmit the time-varying signal from the card to the card reader. The inductive coil 552 is electrically connected to the control circuit 554, which may be integrated into the device processor 314 (FIG. 3). By establishing the configuration in this manner, the inductive coil 552 can be pulsed with

varying currents and current directions so that the time-varying data stream of a card being swiped through the reader is emulated, thus providing the same magnetic data stream to the reader heads of the magnetic stripe reader as would be seen if a card with binary data in multiple spatially distributed data cells 504-516 in the magnetic stripe 502 were swiped through the reader. This magnetic signal will, therefore, emulate the data that would be generated by the swipe of a magnetic stripe card with the desired information embedded in the individual data cells 504-516 of the stripe 502.

[0052] Note that the individual data cells 504-516 are normally empty of data. There are several ways in which the card can be activated so that the data transfer can be started. For example, the card can be initially activated by the authorized user using an on-card "enable button", such as a low-power capacitance sensor, that can be built into the ring of the biometrics sensor 302 (FIG. 3) and used to "wake up" the card when the user is ready to authenticate himself/herself and begin using the card. Authentication of the card user is time stamped for use in determining the length of time to allow transmission of the emulated data. In addition, the magnetic reader 330 (FIG. 3) may have a start sentinel that signals a detector on the card to alert the card that it is in the presence of the card reader 330 (FIG. 3). Once the card is alerted that it is being swiped through the reader 330 (FIG. 3), it begins transmission of the emulated time-varying data from the device processor to the inductive coils 552, thereby generating an exact emulation and transmission to the reader 330 (FIG. 3) of the data that would have been produced by swiping the card through the reader 330 (FIG. 3) with spatially varying data included in the individual data cells 504-516. All such transmission of emulated card data is contingent upon valid biometric authentication of the card user, followed by detection of the card that it is in the presence of the reader head and the reader 330 (FIG. 3) has recognized the start sentinel on the card so that the reader 330 (FIG. 3) is ready to accept the stream of emulated data provided by the device processor. The transmission of data from the device processor 314 (FIG. 3) is suspended once the initial reading of data by the magnetic card reader 330 (FIG. 3) has been completed. This action prevents skimming of card information after the basic transaction has been completed.

[0053] Referring now to FIG. 6, a programmable magnetic card 600 is equipped with inductive coils as illustrated in FIG. 5A or 5B. An on-card biometrics sensor 310 is incorporated to enable positive authentication of the user of the card. This is accomplished by transmitting a biometrics template from the biometrics sensor 310 to the on-card control processor 314 that performs matching operations on the template sent from the biometrics sensor 310 with a template obtained from the authorized user of the card, such authorized template being resident in the control processor 314 (memory 312) from initial registration of the authorized card owner and/or user. Once such biometrics matching has been accomplished, the control processor 314 then authorizes the necessary account numbers and/or card applications to be downloaded into the individual data tracks of the programmable magnetic stripe 308 (magnetic field generator; see also 502 FIGS. 5A and 5B), which then enables the card to be used in standard card-readers throughout the existing world-wide infrastructure.

[0054] Now referring to FIG. 7, a flow chart of an exemplary authentication method 700 for using a device, such as device 300 (FIG. 3), in accordance with the present invention is shown. The device contains information associated with one or more users, a magnetic field generator that is normally inactive and a biometric sensor. The device can be used to enable any type of transaction, such as an access transaction, a control transaction, a financial transaction, a commercial transaction or an identification transaction. The device is normally in standby or sleep mode as shown in block 702. If one or more activation parameters are satisfied, as determined in decision block 704, the device is switched to active mode in block 708. Otherwise, the device remains in standby mode as shown in block 706. The one or more activation parameters may include detecting data from the biometric sensor (e.g., 310 FIG. 3), detecting an external signal from an interface (e.g., 308, 322, 324, 326 FIG. 3) or receiving data from a user interface (e.g., 320 FIG. 3). If authentication data is not received after the device is switched to active mode, as determined in decision block 710, and the active period has timed out, as determined in decision block 712, the device is switched to standby mode in block 714 and again waits for activation parameters in block 704. If, however, the active mode has not timed out, as determined in decision block 712, the device continues to wait for authentication data to be received until the active period has timed out. If, however, authentication data is received from the biometric sensor, as determined in decision block 710, the authentication data is verified in block 716. The verification process determines whether the authentication data is valid for one of the users by comparing the authentication data with a stored biometric template of the one or more users that are authorized or registered to use the device. If the authentication data is not valid, as determined in decision block 718, and the active period has timed out, as determined in decision block 712, the device is switched to standby mode in block 714 and again waits for activation parameters in block 704. If, however, the active mode has not timed out, as determined in decision block 712, the device will again wait for authentication data to be received until the active period has timed out.

[0055] If, however, the authentication data is valid, as determined in decision block 718, the information associated with the authenticated user is accessed in block 720 and provided to the device outputs in block 722. The information can be a simple approval or denial of the transaction, or private information of the user that is required to enable or complete the transaction. As previously described in reference to FIG. 3, the device outputs may include a magnetic field generator 308 (programmable magnetic stripe), a contactless interface 322, a smart card interface 324, or an optical or other I/O interface 326. Using the magnetic field generator 308 for example, this step would involve activating the magnetic field generator 308 and generating a magnetic signal corresponding to the information associated with the authenticated user. In addition, the authentication step (block 716), the information access step (block 720) or the information output step (block 722) may also display information to the user, allow the user to select the information to enable the transaction or allow the user to select the device output or interface to be used. Once the transaction is complete, as determined in decision block 724, the information is cleared from the device output(s) in block 728, the device is switched to standby mode in block 714

and the device waits for various activation parameters in block 704. If, however, the transaction is not complete, as determined in decision block 724 and the process has not timed out, as determined in decision block 726, the process continues to wait for the transaction to be completed. If the process has timed out, as determined in decision block 726, the information is cleared from the device output(s) in block 728, the device is switched to standby mode in block 714 and the device waits for various activation parameters in block 704. The process can be set to interrupt the transaction and deny it if the process times out (e.g., the magnetic field generator has been active for a specified period of time) or the biometric sensor no longer detects the authorized user. Note that this method can be performed by a computer program, such as middleware, embodied in a computer readable medium wherein each step is implemented as one or more code segments, all of which are performed on the card/device.

[0056] Referring now to FIG. 8, one embodiment of an exemplary device 800 for effecting secure physical and commercial transactions in a contactless manner using biometrics is shown. As will be described later in greater detail, the device 800 includes multiple components, such as a biometric sensor 802, a radio frequency ("RF") antenna 804, a controller 806, control buttons 808, a dynamic information display 810, a magnetic information media component 812, and a RF power conversion and power management unit 814. A number of inter-component communications paths 816 provide connections between various components of the device 800.

[0057] The RF antenna 804 may perform multiple functions. For example, it may capture RF energy from a RF field emanated by a RF power source and may also support two-way communication with an associated reader/writer device (not shown). The antenna 804 may be a single antenna capable of performing both functions or may comprise multiple antennae, with one antenna for capturing RF energy from the RF field and another antenna for supporting the two-way communication with the reader/writer device. The communications may include, for example, authenticated identification of a person operating the device 800, various purchases and financial transactions, air ticket booking and airport security check points, and other interactions between the device 800 and the reader/writer device. These communications may be secured using mechanisms such as data encryption. It is understood that other communications components, such as audio or optical components, may replace or supplement the antenna 804. In addition, the antenna 804 may be operable to function with wavelengths other than RF.

[0058] The biometric sensor 802 is used for sensing a physical attribute of a user of the device 800 and generating an analog of this physical attribute. The analog may then be made available to the controller 806. More specifically, the biometric sensor 802 is designed to sense some physical attribute of a person and extract a distinctive analog of that person. To be useful for establishing positive identification, the analog may need to be individualized sufficiently so as to be unique to every person. In addition, a trusted copy—a template—of the analog should be captured. Analogs later sensed by the biometric sensor 802 may then be compared against the template analog. Various physical attributes may

be used for identification purposes, such as fingerprints, voice prints, and retinal or iris prints.

[0059] The controller 806 interacts with the biometric sensor 802 and other components of the device 800 to perform various functions. For example, the controller 806 may capture the analog of the physical attribute for long term storage as a trusted template analog of an authorized user, as well as for immediate comparison to a stored trusted template analog during an authentication procedure. The controller 806 may also determine whether the comparison indicates a match between the template analog and the analog captured by the biometric sensor 802. In addition, the controller 806 may control the dynamic information display 810, respond to input from the control buttons 810, and control the magnetic information media component 812. Furthermore, the controller 806 may support two-way communications with an associated reader/writer device (FIG. 9) via the RF antenna 804. The controller may be a single controller/processor or may comprise multiple controllers/processors.

[0060] The dynamic information display 810 may be used to display information to a user, as well as to enable a process with which the user may interact using the control buttons 810. The magnetic information media component 812 may be manipulated so that it provides information via a magnetic field. The RF power unit 814 may convert RF radio energy to electrical energy, and may control storage and distribution of the electrical energy to the other components in the device 800. It is understood that the device 800 may also have a battery and/or other power means to use as a backup or alternative power source for the RF power control unit 814.

[0061] Referring now to FIG. 9, the device is illustrated in an exemplary environment 900 that enables contactless interaction with a reader/writer device 902. To achieve this contactless interaction, the device 800 is shown with the antenna 804, as described in reference to FIG. 8. The device 902 uses one or more antennae 903 to communicate with device 800, as well as emanate a RF field 906 with the purpose of supplying power to compatible devices, such as device 800. In operation, a two-way communication link 908 may be established between the reader/writer device 902 and the device 800.

[0062] It is understood that many different reader/writer configurations may be used. For example, the reader/writer device 902 may be in communication with other devices or with a network. Furthermore, the reader/writer device 902 may be in communication with other devices or with a network. Furthermore, the reader/writer device 902 may include the RF power source, or they may be separate devices. For the purposes of clarity, the reader/writer device 902 of the present invention example includes the RF power source, although alternate sources of RF power may be used.

[0063] Referring to FIG. 10 and with continued reference to FIGS. 8 and 9, the device 800 may be operated in the environment 900 using a method 1000 as follows. In step 1002, the device 800 is placed into the RF field 906 emanated by the reader/writer device 902. When placed into the RF field, the device 800 captures power from the RF field 906, which powers up the device's 800 electronics. In step 1004, the biometric sensor 802 is actuated by a user. The method of actuation may depend on the type of biometric

sensor (e.g., a fingerprint for a fingerprint sensor, speaking for a voice sensor, etc.). In step 1006, an authentication process is performed by the device 800. As in the previous step, the authentication process may depend on the type of biometric sensor. For example, the detected fingerprint or voice may be compared to a template in the memory of the device 800. In step 1008, a determination is made as to whether the user is authenticated. If the authentication process fails to validate the user, the method 1000 may return to step 1004. If the user is validated by the authentication process, the method continues to step 1010, where the device 800 continues the desired transaction with the reader/writer device 902. Once this occurs, the device 800 may be removed from the RF field 906 in step 1012, which powers down the device 800.

[0064] Referring now to FIG. 11, in another embodiment, a device 1100 illustrates an implementation of the present disclosure using a form factor similar to that of a credit card. The credit card form factor of the device 1100 includes several components, such as a fingerprint sensor 1102, a RF antenna 1104, a first controller 1106, a second controller 1108, function selector buttons 1110, an electro-luminescent display 1112 and a magnetic strip 1114. In the present example, the first controller 1106 is an application specific integrated circuit ("ASIC") chip and the second controller is a smart card chip, although it is understood that the functionality of both controllers may be provided by a single controller.

[0065] The ASIC 1106 is a custom integrated circuit chip developed for use in the device 1100. The ASIC 1106 includes Random Access Memory ("RAM") which may be used for temporarily storing a current fingerprint analog detected by the fingerprint sensor 1102 and for temporarily storing intermediate results of processing calculations (e.g., fingerprint comparisons, etc.). The ASIC 1106 may also include non-volatile memory (e.g., Flash memory or EEPROM) to store and retrieve one or more fingerprint template analogs that are used for comparison against the current fingerprint analog.

[0066] Circuitry contained within the ASIC 1106 provides an interface between the ASIC 1106 and the fingerprint sensor 1102. In the present example, the ASIC 1106 contains a microprocessor core with dedicated program and temporary memory, enabling the ASIC 1106 to use an array of processing elements for executing instructions stored with the ASIC 1106 in parallel. The instructions enable the ASIC 1106 to perform a comparison between the current fingerprint analog and a template fingerprint analog. Other instructions included within the ASIC 1106 may provide support for an authorization signal to be sent to the smart card 1108 after an authentication process has been completed. In addition, the ASIC 1106 may be used to drive the electro-luminescent display 1112, read the function control buttons 1110, and drive the programmable magnetic strip 1114.

[0067] The smart card chip 1108 may support various application programs. These applications may include, for example, storage/retrieval of personal demographics information, storage/retrieval of a digitized picture of the cardholder, an "electronic purse" functionality, financial transactions, purchases, etc. In addition, the smart card chip 1108 may support two-way communication data transfers and may perform various encryption functions to support secure

communications. In the present example, the communications and encryption are based on known standards, but proprietary protocols may be used if desired. It is envisioned that the smart card chip 1108 may support smart card interactions such as identification validation, credit card transactions, and others. Note that the control and processing functions of the device 1100 can be handled by the ASIC 1106, the smart card chip 1108, any combination of the ASIC 1106 and the smart card chip 1108, or a single chip.

[0068] The fingerprint sensor 1102 is designed to detect fingerprint information and provide the detected information to other components of the device 1100. In the present example, the fingerprint sensor 1102 comprises a polymer thick film ("PTF") construction, which provides the fingerprint sensor 1102 with the flexibility and ruggedness needed for implementation on the device 1100. As described in greater detail below in FIGS. 12 and 10, the fingerprint sensor 1102 comprises a matrix of points that are operable to detect high and low points corresponding to ridges and valley of a fingerprint. The points are captured and used by the ASIC 1106 to determine whether the detected fingerprint analog matches a fingerprint template analog that is stored in memory.

[0069] Referring now to FIG. 12, in one embodiment, the PTF sensor 1102 comprises a rectangular arrangement of row electrodes 1202 and column electrodes 1204. It is noted that more or fewer columns and rows may be included in the PTF sensor 1102, depending on such factors as the desired resolution of the PTF sensor 1102 (e.g., the number of data points desired). Electrical connections from the row and column electrodes 1202, 1204 may route to the ASIC 1106.

[0070] In operation, a fingerprint analog detected by the PTF sensor 1102 may be captured by the ASIC 1106 as a sequence of numerical values. For purposes of illustration, the row and column electrodes 1202, 1204 may be viewed as a two dimensional matrix of pixels, with numerical values representing intersections between the row and column electrodes. The numerical values may be associated with gray scale values, and an analog representing a fingerprint may be generated from the matrix of gray scale values. It is understood that there is no need to transform the captured analog into a visible image since the matching between the stored template fingerprint analog and the candidate fingerprint analog need not rely on a visual process. However, it is convenient to conceptualize the numerical values as an image for purposes of evaluating the sensor resolution used to support fingerprint authentication. It is generally accepted that a graphical resolution of from 100 dots per inch ("dpi") to 500 dpi is sufficient for fingerprint authentication. In the present example, the PTF sensor 1102 comprises 200 row electrodes and 200 column electrodes arranged in a ½" by ½" matrix, which corresponds to a graphical resolution of 400 dpi.

[0071] Referring now to FIG. 13A, a schematic depiction of functional layers of one embodiment of the PTF sensor 1102 of FIG. 11 is shown. The PTF sensor 1102 is comprised of functional layers including an annularly shaped topside electrode 1302; an insulator with backside reflector 1304; and electro-luminescent layer 1306; insulator layers 1308, 1312, 1316, and 1320; row electrodes 1310; column electrodes 1314; an electro-resistive layer 1318; and elec-

trode 1322; and a substrate layer 1324. The substrate layer 1324 may be a portion of the substrate for the entire device 1100.

[0072] In operation, when a user of the device 1100 places a finger or thumb (henceforth only finger will be specified, although it is understood that both fingers and thumb are intended) on the surface of the PTF sensor 1102, the finger contacts the topside electrode 1302 and becomes electrically grounded to the topside electrode 1302. When a voltage is applied to row electrodes 1310, and electric field is generated between the row electrodes 1310 and the topside electrode 1302. The strength of the generated field varies depending on how close the finger is to the topside electrode 1302. For example, fingerprint ridges may be relatively close to the topside electrode 1302 of the PTF sensor 1102, varying the generated field in a detectable manner. Fingerprint valleys may be more distant from the PTF sensor 1102 than the fingerprint ridges, which may vary the generated field in a detectable manner that may be differentiated from the variations caused by the fingerprint ridges.

[0073] The electro-luminescent layer 1306 may emit more or less light as the electric field that impinges upon it varies, thereby generating an analog of the fingerprint incident upon the PTF sensor 1102. The reflector component of the insulator with backside reflector layer 1304 serves to reflect the omni directional light emitted by the electro-luminescent layer 1306 and thus intensify the fingerprint analog. The PTF sensor 1102 may be operated by applying a bias voltage to only one row electrode at a time, successively biasing and unbiasing one row after another. This has the effect of causing the electro-luminescent layer 1306 to generate an analog of an elongated thin strip of the fingerprint. By sensing each of these analogs and combining them upon completion of row sequencing, a complete analog may be collected.

[0074] It is a property of the electro-resistive layer 1318 that when it is placed in an electrical field its resistance varies with the intensity of light incident upon it. The light emitted by the electro-luminescent layer 1306, which is an analog of the fingerprint, passes through the intervening layers 1308, 1310, 1312, 1314, and 1316 to impinge upon the electro-resistive layer 1318. The electro-resistive layer 1318 is placed in an electric field by placing a DC voltage bias on the electrode 1322 relative to the column electrodes 1314, causing the electro-resistive layer to exhibit varying resistance depending upon the intensity of light incident upon it and thereby forming an analog of the fingerprint. A voltage is applied to the column electrodes 1314, and the impedance between the column electrodes 1314 and the electrode 1322 can be measured. This measured impedance is directly related to the varying resistance of the electro-resistive layer 1318 and hence an analog of the fingerprint. So by activating each row electrode in succession, as described above, an analog of the fingerprint can be captured and stored.

[0075] The ASIC 1106 may control the sequential activation of the row electrodes 1310, the reading back of the varying resistance from the column electrodes 1314, and other functions of the PTF sensor 1102. It is understood that other approaches may be used, such as reading one column at a time for each row or reading multiple row/columns at once. Furthermore, while the preceding description focuses

on the use of the PTF sensor 1102 as a fingerprint sensor, the principle of operation of the PTF sensor 1102 is general and not limited to capturing fingerprint analogs.

[0076] Referring now to FIG. 13B, one embodiment of a portion of the device 1100 illustrates the biometric sensor 1102, display 1112, and RF antenna 1104 formed on the substrate 1324. The biometric sensor includes layers 1302-1322 as described with respect to FIG. 10, the display 1112 comprises layer 1326-1336, and the RF antenna comprises layers 1338-1348. As is illustrated in FIG. 13B, each of the components 1102, 1112, 1104 share a number of layers (e.g., 1322, 1336, and 1348). This sharing simplifies the design of the device 1100 and may also reduce manufacturing costs.

[0077] Referring again to FIG. 11, the RF antenna 1104, which may include one or more antennae, may capture RF energy from a RF field emanated by a RF power source and may also support two-way communication with an associated reader/writer device (not shown). The RF energy which is captured is converted to electrical energy and accumulated within the device 1100. In some embodiments of the device 1100, a rechargeable battery may power the electronic components when no RF energy field is present. Such a battery may be charged via a RF energy field or alternative charging means.

[0078] The electro-luminescent display 1112 provides the capability to display information to a user of the device 1100. For example, the information may include a credit card number to support "card not present" transactions, a residual balance of an "electronic purse," air travel flight and seat assignment information, and similar information. Furthermore, interaction with the display 1112 may be accomplished via the function control buttons 1110. For example, the buttons 1110 may be used to select a credit card number (if the device 1100 stores multiple numbers) viewed via the display 1112 or to enter a personal identification number. The pliability of the electro-luminescent display 1112 aids its use in the card-like form factor of the device 1100. While two control buttons 1110 are illustrated, it is understood that other numbers and configurations of function control buttons may be used.

[0079] A dynamic magnetic strip 1114 is provided to provide compatibility with existing reader devices. The dynamic magnetic strip 1114 may be used in either fixed or dynamic mode. In dynamic mode, magnetically stored information—such as a credit card number—may be changed under control of the ASIC 1106.

[0080] Referring now to FIG. 14, an illustrative power circuit 1400, such as may be used in the device 1100 of FIG. 11, is depicted. When appropriate RF energy is incident upon the device 1100, the RF energy couples into a RF antenna 1402. From the antenna 1402, the energy enters a RF-to-DC power converter 1404, which includes a full-wave rectifier to convert the AC RF field into a DC-like circuit. Capacitance may be provided to buffer the AC peak variations into a DC-like source. The intermediate power generated by this process may be used for a variety of purposes, such as charging a battery 1406 if the battery 1406 is below its full capacity and feeding power to the device 1100. The battery 1406 may be charged through a battery management unit 1408. A smart power multiplexer 1410 may be used to determine whether to draw power from the battery management unit 1408, directly from the RF-to-DC power converter 1404, or from both.

[0081] A voltage regulator 1412 creates a stable DC voltage level to power the device 1100. When no RF energy is coupled into the RF antenna 1402, the RF-to-DC converter 1404 may not function and power may be drawn from the battery management unit 1408 by the smart power multiplexer 1410. As before, the voltage regulator 1112 creates a stable DC voltage level to power the device 1100. It is understood that, in other embodiments, the power circuit 1400 may not employ a battery or rechargeable battery, and may rely solely on power captured from the RF field.

[0082] Referring now to FIG. 15, an exemplary template storage method 1500 illustrates one embodiment for capturing and storing a template of a fingerprint analog for the device 1100 of FIG. 11. In step 1502, a user places the device 1100 in a RF field emanated by a reader/writer device. As described previously, the device 1100 captures power from the RF field. In step 1504, the user places his thumb or finger on the finger print sensor 1102 and, in step 1506, the device 1100 determines whether a template fingerprint analog is already stored. If it is determined that no template fingerprint analog is stored, the method 1500 continues to step 1508. In step 1508, the user's incident fingerprint is sensed by the fingerprint sensor 1102, a fingerprint analog is generated by the fingerprint sensor 1102, and the ASIC 1106 stores the fingerprint analog as a template fingerprint analog. If a fingerprint template analog is already stored, the method 1500 continues to step 1510, where the device 1100 is removed from the RF field. It is understood that other events may occur before step 1510 if a fingerprint template analog is already stored, such as illustrated in FIG. 16.

[0083] Although not shown in the present example, multiple template fingerprint analogs may be stored in the device 1100. The template fingerprint analogs may represent multiple fingerprints of a single person or may represent the fingerprints of different people. This may be accomplished, for example, by implementing a method for allowing the device 1100's owner to securely control initialization of multiple template fingerprint analogs and to selectively engage which template fingerprint analog will be used to authenticate identity and authorize transactions. Alternately, if the device 1100 is to be used in environments requiring higher security, the user of the device 1100 may need to appear in person and validate his or her identify using traditional methods (e.g., a driver's license, birth certificate, etc.). After validation, the user's template fingerprint analog may be placed into the device 1000 as described above or through other means (e.g., a scanner that transfers the template fingerprint analog into the device 1000).

[0084] Referring now to FIG. 16, in another embodiment, a method 1600 illustrates one method of operation for the device 1100. In step 1602, as has been described previously, the device 1100 is placed into a RF field emanated by a reader/writer device. When placed into the RF field, the device 1100 captures power, energizing its electronics. In step 1604, a user places one of his fingers onto the fingerprint sensor 1102. As described above, the fingerprint sensor 1102 captures an analog of the fingerprint and passes the analog to the SAIC 1106.

[0085] In step 1606, an authentication process is performed by comparing the captured fingerprint analog to one

or more template fingerprint analogs stored in memory. In step 1608, a determination is made as to whether the user is authentication (e.g., whether the captured fingerprint analog matches a stored template fingerprint analog). If the authentication process fails to validate the user, the method 1600 may return to step 1604 as shown or may end, requiring the user to remove the device 1100 from the RF field and begin again with step 1602. If the user is validated by the authentication process, the method continues to step 1610, where the device 1100 conducts a communications handshake process with the reader/writer device via a contactless two-way communication link. In step 1612, the device 1100 continues the desired transaction with the reader/writer device. Once this occurs, the device 1100 may be removed from the RF field, which powers down the device 1100.

[0086] Referring now to FIG. 17, in another embodiment, a method 1700 illustrates using the present disclosure in an air transportation environment. A traveler desiring to make a remote reservation presents a device (such as the device 800 of FIG. 8) to a reader/writer device. In the present example, the reader/writer device is attached to a personal computer ("PC") via a wired or wireless connection. The PC may enable the traveler to access an application, such as a web based flight reservation application.

[0087] In step 1702, a determination is made as to whether the traveler has selected a remote reservation and ticketing process. If the traveler has selected such a process, the method 1700 continues to step 1704, where the device 800 is used in conjunction with PC and the reader/writer to verify the traveler's identification and approve the transaction and associated payments. In addition, flight information may be transferred from the reader/writer device into the device 800.

[0088] The method 1700 then continues to step 1706, where a determination is made as to whether the traveler has selected to remotely check-in baggage. If the traveler has not selected to remotely check-in baggage, the method 1700 continues to step 1712. If the traveler has selected to remotely check-in baggage, the method 1700 continues to step 1708, where the device 800 is used in conjunction with PC and the reader/writer to verify the traveler's identification. In addition, flight and ticket information may be read from the device 800 to further automate the baggage check-in process. After the traveler has entered any desired information (e.g., number of bags, etc.), baggage reference information may be transferred into the traveler's device 800 for later transfer into and use by the airline's ticketing and baggage tracking systems.

[0089] Returning to step 1702, if it is determined that the traveler has not selected a remote reservation and ticketing process, the method 1700 continues to step 1710, where the traveler may use the device 800 with a reader/writer device at a counter or self-service kiosk in a manner similar to the process of the remote check-in of step 1704. More specifically, the traveler may use the device 800 to verify the traveler's identification and approve a purchase transaction, as well as any associated payments. In addition, flight information may be transferred from the reader/writer device into the device 800.

[0090] Continuing to step 1712, the traveler may use the device 800 with the reader/writer device at the counter or self-service kiosk in a manner similar to the process of the remote baggage check-in of step 1708. More specifically, the

traveler may use the device 800 to verify the traveler's identification, provide flight and ticket information, and store baggage reference information that is transferred from the reader/writer device.

[0091] After the ticketing and baggage check-in, the method 1700 continues to steps 1714, 1716, and 1718, where the traveler may present the device 800 to other reader/writer devices for identification and ticket authentication. For example, this may occur at security checkpoints, gates, and/or at boarding. It is understood that some of the reader/writer devices may be in communication with airline and/or government databases.

[0092] Referring now to FIG. 18, in another embodiment, a method 1800 illustrates using the present disclosure in a health care environment. In step 1802, a determination is made as to whether a patient desires to perform a pre check-in process before arriving at a healthcare facility. If it is determined that the patient does desire to perform a pre check-in process, the method 1800 continues to step 1804, where the patient may present a device (such as the device 800 of FIG. 8) to a reader/writer device. In the present example, the reader/writer device is attached to a personal computer via a wired or wireless connection. The PC may enable the patient to access an application, such as a web-based healthcare application. Upon presentation of the device in step 1804, the patient may be identified, payment and care instructions may be approved, and medical information (e.g., records, prescriptions, etc.) may be activated. The device 800 may also be used to provide the patient with medical alerts.

[0093] In step 1806, if the patient has not performed the pre check-in process of step 1804, the patient may use the device 800 to perform similar functions at the healthcare facility. The method then continues to step 1808, where the device may be used to access provider services. For example, the device 800 may be used to interact with a reader/writer device at a desk or workstation in the healthcare facility (e.g., an examination room). This interaction may authenticate the patient's identification, provide access to pertinent medical records, verify that the records are updated, and store one or more prescriptions.

[0094] Continuing to step 1810, the patient may present the device 800 to a reader/writer device at a pharmacy. The device 800 may be used to authenticate the patient's identification for a prescription and provide the prescription to the pharmacy. Furthermore, the device 800 may provide insurance/payment information and enable the patient to approve the transaction.

[0095] Referring now to FIGS. 19 and 20, in another embodiment, methods 1900 and 2000 illustrate using the present disclosure in a financial transaction environment. The financial transaction environment includes making retail purchases in either a physical store or on-line (e.g., over the Internet). The present disclosure may be implemented in the financial transaction environment by using a device, such as the device 800 of FIG. 8, to identify buyers, verify the identity of the buyer rapidly in a localized venue, associate the buyer's identity with a credit or debit account, and/or assure the availability and legitimacy of funds in these accounts for payment transactions.

[0096] Payments for retail purchases are generally accomplished in one of three ways: with cash; with a check; or with

a credit or debit card. In a cash transaction, there is generally no need for validating the identification of the buyer. In a transaction where a check is used, there generally is a need for identification of the buyer. This identification may occur by way of the buyer's presentation of a driver's license or alternate, approved identification card, presentation of a credit card to indicate credit-worthiness, or by a telecommunication connection to check security processing service to assure fund availability for, and legitimacy of, the check presented for payment.

[0097] In a transaction where a credit or debit card is used, there are generally various procedural mechanisms in place to assure buyer identification and legitimate ownership of the card presented for the payment transaction. For example, the payment may require the entry of numeric PIN ("Personal Identification Number") security code by the buyer and assumed owner of the card. Alternatively, sales personnel may compare the buyer's signature on the back of the card presented for payment versus the requested signature on the purchase receipt provided for the goods or services purchased. In some cases, cards have a photograph of the card owner on them, and sales personnel may make cursory comparisons of this photograph with the buyer to establish identification. However, both photographic comparison and PIN-based card authorization have weaknesses for assuring identification, and both have potential risk for fraudulent processing. Photographs can be falsified and PIN numbers can be stolen. In the case of on-line purchases, buyers are not present to provide authorizing signatures, photographic comparisons cannot be made with existing processing infrastructure, and PIN-based transactions can be compromised with identity theft.

[0098] Referring specifically to FIG. 19, before the device 800 is usable in financial transactions, it should be initialized by the buyer/owner with the registration of a selected fingerprint pattern into secured memory of the device 800. To register a selected fingerprint, the device owner holds the device 800 in the RF field generated by a point of sale ("POS") device, which may be a kiosk, personal computer, cash register, or similar device. The RF energy from the POS device provides for the power of the device 800 and display activation in step 1902. In step 1904, a determination is made as to whether the device 800 has been previously used. For example, the device 800 may determine if a fingerprint template analog is already stored in memory. If the device 800 has been previously used, the method 1900 ends. If the device has not been previously used, the device 800 continues to step 1906, where the owner is prompted to actuate the biometric sensor. For example, this may entail the owner briefly touching the biometric sensor 802 on the device 800 with a selected finger or thumb. The fingerprint information is read from the biometric sensor 802 and stored in the device 800 in steps 1908, 1910 while the owner maintains contact with the biometric sensor 802. The owner may maintain contact with the biometric sensor 802 until, in step 1912, an acknowledgement is displayed on the display 800 that the fingerprint pattern has been successfully registered in the device 800 as an encrypted template.

[0099] Referring specifically to FIG. 20, to authorize a payment transaction where invoice information is displayed by the POS device, the user of the device 800 holds the device 800 within a RF field generated by a RF reader connected to the POS device in step 2002. For example, the

user may hold the device 810 at an approximate six inch distance from the RF reader. In step 2004, the user actuates the biometric sensor 802 (e.g., touches the fingerprint sensor with his/her finger or thumb) to effect a comparative match with his/her previously registered fingerprint securely stored in the memory of the card. A successful match effects an encrypted approval and transfer of cardholder account data to the seller's administrative account receivables processing system.

[0100] In step 2006, a determination is made as to whether the user desires to transfer electronic receipt information to the device 800. If not, the method 2000 continues to step 2010, where the device 800 is removed from the RF field. If it is determined in step 2006 that the user does want to transfer electronic receipt information to the device 800, the method 2000 continues to step 2008, where the device 800 stores the information in memory. The method 2000 may then continue to step 2008, where the device 800 is removed from the RF field.

[0101] While the preceding description shows and describes one or more embodiments, it will be understood by those skilled in the art that various changes in form and entail may be made therein without departing from the spirit and scope of the present disclosure. For example, the present disclosure may be implemented in a variety of form factors, such as a wristwatch or wristwatch band, a key ring, or a variety of other physical structures. Therefore, the claims should be interpreted in a broad manner, consistent with the present disclosure.

What is claimed is:

1. An apparatus comprising:
 - a substrate;
 - a magnetic field generator disposed within the substrate that is normally inactive;
 - a biometric sensor mounted on the substrate;
 - a memory disposed within the substrate;
 - a processor disposed within the substrate and communicably coupled to the magnetic field generator, the biometric sensor and the memory, wherein the processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified; and
 - a power source disposed within the substrate and electrically connected to the magnetic field generator, the biometric sensor and the processor.
2. The apparatus as recited in claim 1, wherein the magnetic field generator creates a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader.
3. The apparatus as recited in claim 1, wherein the magnetic field generator comprises a programmable magnetic stripe.
4. The apparatus as recited in claim 3, wherein the programmable magnetic stripe comprises:
 - a magnetic stripe either mounted on the substrate or disposed within the substrate;
 - one or more induction coils disposed within the substrate underneath the magnetic stripe; and

a controller disposed within the substrate that is connected to the one or more induction coils and operable to generate a spatially varying or time-varying magnetic signal via the one or more induction coils and the magnetic stripe.

5. The apparatus as recited in claim 4, wherein the magnetic signal includes binary data describing a user name, user number and apparatus expiration date.

6. The apparatus as recited in claim 4, wherein the magnetic stripe contains three-tracks and each track contains a set of magnetic data cells.

7. The apparatus as recited in claim 1, wherein the processor comprises a smart card processor and an ASIC chip.

8. The apparatus as recited in claim 1, wherein the power source is controlled by a power management unit.

9. The apparatus as recited in claim 1, wherein the power source is selected from the group consisting of a battery, a piezoelectric generator, a solar panel, an electromagnetic energy converter; a kinetic energy converter and combinations thereof.

10. The apparatus as recited in claim 1, wherein the power source comprises:

- a battery;
- a power generator;
- a converter electrically connected to the power generator and operable to convert power received from the power generator into power usable by the apparatus or to charge the battery;
- a battery management unit connected to the battery; and
- a power multiplexer connected to the battery management unit and the converter and operable to determine whether to draw power from the battery management unit, from the converter, or from both.

11. The apparatus as recited in claim 1, wherein the biometric sensor is selected from the group consisting of a fingerprint sensor, retina sensor, iris sensor or voice sensor.

12. The apparatus as recited in claim 1, wherein the biometric sensor comprises a matrix of points operable to detect high and low points corresponding to ridges and valleys of a fingerprint.

13. The apparatus as recited in claim 1, wherein the biometric sensor comprises an emitter and a detector wherein light projected by the emitter is reflected from a user's finger onto the detector.

14. The apparatus as recited in claim 1, further comprising a user interface mounted on the substrate that is communicably coupled to the processor and electrically connected to the power source.

15. The apparatus as recited in claim 14, wherein the user interface is selected from the group consisting of a touch pad, one or more buttons, a display and a voice sensor.

16. The apparatus as recited in claim 1, further comprising an output interface mounted on the substrate that is communicably coupled to the processor and electrically connected to the power source.

17. The apparatus as recited in claim 16, wherein the output interface is selected from the group consisting of an antenna for wireless communication and an optical transmitter.

18. The apparatus as recited in claim 1, further comprising a smart card interface mounted on the substrate that is

communicably coupled to the processor and electrically connected to the power source.

19. The apparatus as recited in claim 1, further comprising a contactless interface disposed within the substrate that is communicably coupled to the processor and electrically connected to the power source.

20. The apparatus as recited in claim 19, wherein the contactless interface is selected from the group consisting of an antenna for wireless communication and an optical transceiver.

21. The apparatus as recited in claim 1, wherein the substrate is semi-flexible.

22. The apparatus as recited in claim 1, wherein the substrate is integrated into a card selected from the group consisting of an access card, a credit card, a debit card, an identification card, a mini-card, a security card, a stored value card and a vendor-specific card.

23. The apparatus as recited in claim 1, wherein the substrate is integrated into a travel credential selected from the group consisting of a passport, an immigration card and a visa.

24. The apparatus as recited in claim 1, wherein the substrate is integrated into a personal communication device selected from a group consisting of a personal data assistant, a telecommunications device, a pager, a computer and an electronic mail transceiver.

25. The apparatus as recited in claim 1, wherein the substrate is integrated into a personal device/belonging selected from a group consisting of a watch, a jewelry, a key ring, a tag and eye glasses.

26. The apparatus as recited in claim 1, wherein the processor and the memory are integrated into a single integrated circuit.

27. The apparatus as recited in claim 1, wherein the memory contains a biometric analog of a user.

28. The apparatus as recited in claim 1, wherein the processor provides binary data to the magnetic field generator after a user has been authenticated using the biometric sensor.

29. The apparatus as recited in claim 1, wherein the processor deactivates the magnetic field generator after the magnetic field generator has been active for a specified period of time.

30. The apparatus as recited in claim 1, wherein the processor deactivates the magnetic field generator when the biometric sensor no longer detects the authorized user.

31. A method for enabling a transaction using an apparatus containing information associated with one or more users, a magnetic field generator that is normally inactive and a biometric sensor, the method comprising the steps of:

receiving authentication data from the biometric sensor;

determining whether the authentication data is valid for one of the users; and

activating the magnetic field generator and generating a magnetic signal corresponding to the information associated with the authenticated user whenever the authentication data is valid.

32. The method as recited in claim 31, wherein the information associated with the authenticated user enables approval of the transaction.

33. The method as recited in claim 31, further comprising the step of activating the magnetic field generator and

generating a magnetic signal that enables denial of the transaction whenever the authentication data is not valid.

34. The method as recited in claim 31, further comprising the step of receiving one or more activation parameters.

35. The method as recited in claim 34, wherein the one or more activation parameters includes detecting data from the biometric sensor, detecting an external signal or receiving data from a user interface.

36. The method as recited in claim 31, wherein the transaction is an access transaction, a control transaction, a financial transaction, a commercial transaction or an identification transaction.

37. The method as recited in claim 31, wherein the step of determining whether the authentication data is valid comprises comparing the authentication data to one or more biometric templates stored on the device.

38. The method as recited in claim 31, wherein the magnetic signal is a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader.

39. The method as recited in claim 31, further comprising the step of deactivating the magnetic field generator after the magnetic field generator has been active for a specified period of time.

40. The method as recited in claim 31, further comprising the step of deactivating the magnetic field generator when the biometric sensor no longer detects the authorized user.

41. The method as recited in claim 31, further comprising the step of selecting the information to enable the transaction.

42. The method as recited in claim 31, wherein the magnetic signal is a time-varying magnetic signal for emulating the data obtained from swiping a magnetic stripe card through a magnetic card reader.

43. The method as recited in claim 31, further comprising the step of displaying information to the user.

44. The method as recited in claim 31, further comprising the step of transmitting the information associated with the user via a wireless communications antenna.

45. The method as recited in claim 31, further comprising the steps of:

receiving power from an external power source in a contactless manner; and

converting the power received from the external power source into power compatible with the apparatus.

46. A computer program embodied in a computer readable medium for enabling a transaction using an apparatus containing information associated with one or more users, a magnetic field generator that is normally inactive and a biometric sensor, the computer program comprising:

a code segment for receiving authentication data from the biometric sensor;

a code segment for determining whether the authentication data is valid for one of the users; and

a code segment for activating the magnetic field generator and generating a magnetic signal corresponding to the information associated with the authenticated user whenever the authentication data is valid.

47. The computer program as recited in claim 46, wherein the information associated with the authenticated user enables approval of the transaction.

48. The computer program as recited in claim 46, further comprising a code segment for activating the magnetic field generator and generating a magnetic signal that enables denial of the transaction whenever the authentication data is not valid.

49. The computer program as recited in claim 46, further comprising a code segment for receiving one or more activation parameters.

50. The computer program as recited in claim 49, wherein the one or more activation parameters includes detecting data from the biometric sensor, detecting an external signal or receiving data from a user interface.

51. The computer program as recited in claim 46, wherein the transaction is an access transaction, a control transaction, a financial transaction, a commercial transaction or an identification transaction.

52. The computer program as recited in claim 46, wherein the code segment for determining whether the authentication data is valid comprises comparing the authentication data to one or more biometric templates stored on the device.

53. The computer program as recited in claim 46, wherein the magnetic signal is a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader.

54. The computer program as recited in claim 46, further comprising a code segment for deactivating the magnetic field generator after the magnetic field generator has been active for a specified period of time.

55. The computer program as recited in claim 46, further comprising a code segment for deactivating the magnetic field generator when the biometric sensor not longer detects the authorized user.

56. The computer program as recited in claim 46, further comprising a code segment for selecting the information to enable the transaction.

57. The computer program as recited in claim 46, wherein the magnetic signal is a time-varying magnetic signal for emulating the data obtained from swiping a magnetic stripe card through a magnetic card reader.

58. The computer program as recited in claim 46, further comprising a code segment for displaying information to the user.

59. The computer program as recited in claim 46, further comprising a code segment for transmitting the information associated with the user via a wireless communications antenna.

60. A system comprising:

- one or more user devices, each user device comprising
 - a substrate,
 - a magnetic field generator disposed within the substrate that is normally inactive,
 - a biometric sensor mounted on the substrate,
 - a memory disposed within the substrate,
 - a device processor disposed within the substrate and communicably coupled to the magnetic field generator, the biometric sensor and the memory, wherein the processor is operable to process biometric information received from the biometric sensor to verify that a user is authorized to use the apparatus and activate the magnetic field generator when the user is verified, and

- a power source disposed within the substrate and electrically connected to the magnetic field generator, the biometric sensor and the device processor;

- one or more system interfaces operable to communicate with the user device; and

- a system processor communicably coupled to the one or more system interfaces.

61. The system as recited in claim 60, wherein the one or more system interfaces includes an optical interface, a smart card interface, a wireless communication interface, a magnetic reader, an initialization interface or a recharger.

62. The system as recited in claim 60, further comprising a database communicably coupled to the system processor.

63. The system as recited in claim 60, further comprising one or more remote computers communicably coupled to the system processor via a network.

64. The system as recited in claim 60, wherein the magnetic field generator creates a time-varying magnetic signal for emulating data obtained from swiping a magnetic stripe card through a magnetic card reader.

65. The system as recited in claim 60, wherein the magnetic field generator comprises a programmable magnetic stripe.

66. The system as recited in claim 65, wherein the programmable magnetic stripe comprises:

- a magnetic stripe either mounted on the substrate or disposed within the substrate;

- one or more induction coils disposed within the substrate underneath the magnetic stripe; and

- a controller disposed within the substrate that is connected to the one or more induction coils and operable to generate a magnetic signal via the one or more induction coils and the magnetic stripe.

67. The system as recited in claim 66, wherein the magnetic signal includes binary data describing a user name, user number and apparatus expiration date.

68. The system as recited in claim 66, wherein the magnetic stripe contains three-tracks and each track contains a set of magnetic data cells.

69. The system as recited in claim 60, wherein the device processor comprises a smart card processor and an ASIC chip.

70. The system as recited in claim 60, wherein the power source is controlled by a power management unit.

71. The system as recited in claim 60, wherein the power source is selected from the group consisting of a battery, a piezoelectric generator, a solar panel, an electromagnetic energy converter; a kinetic energy converter and combinations thereof.

72. The system as recited in claim 60, wherein the power source comprises:

- a battery;

- a power generator;

- a converter electrically connected to the power generator and operable to convert power received from the power generator into power usable by the apparatus or to charge the battery;

- a battery management unit connected to the battery; and

a power multiplexer connected to the battery management unit and the converter and operable to determine whether to draw power from the battery management unit, from the converter, or from both.

73. The system as recited in claim 60, wherein the biometric sensor is selected from the group consisting of a fingerprint sensor, retina sensor, iris sensor or voice sensor.

74. The system as recited in claim 60, wherein the biometric sensor comprises a matrix of points operable to detect high and low points corresponding to ridges and valleys of a fingerprint.

75. The system as recited in claim 60, wherein the biometric sensor comprises an emitter and a detector wherein light projected by the emitter is reflected from a user's finger onto the detector.

76. The system as recited in claim 60, further comprising a user interface mounted on the substrate that is communicably coupled to the device processor and electrically connected to the power source.

77. The system as recited in claim 76, wherein the user interface is selected from the group consisting of a touch pad, one or more buttons, a display and a voice sensor.

78. The system as recited in claim 60, further comprising an output interface mounted on the substrate that is communicably coupled to the device processor and electrically connected to the power source.

79. The system as recited in claim 78, wherein the output interface is selected from the group consisting of an antenna for wireless communication and an optical transmitter.

80. The system as recited in claim 60, further comprising a smart card interface mounted on the substrate that is communicably coupled to the device processor and electrically connected to the power source.

81. The system as recited in claim 60, further comprising a contactless interface disposed within the substrate that is communicably coupled to the device processor and electrically connected to the power source.

82. The system as recited in claim 81, wherein the contactless interface is selected from the group consisting of an antenna for wireless communication and an optical transceiver.

83. The system as recited in claim 60, wherein the substrate is semi-flexible.

84. The system as recited in claim 60, wherein the substrate is integrated into a card selected from the group consisting of an access card, a credit card, a debit card, an identification card, a mini-card, a security card, a stored value card and a vendor-specific card.

85. The system as recited in claim 60, wherein the substrate is integrated into a travel credential selected from the group consisting of a passport, an immigration card and a visa.

86. The system as recited in claim 60, wherein the substrate is integrated into a personal communication device selected from a group consisting of a personal data assistant, a telecommunications device, a pager, a computer and an electronic mail transceiver.

87. The system as recited in claim 60, wherein the substrate is integrated into a personal device/belonging selected from a group consisting of a watch, a jewelry, a key ring, a tag and eye glasses.

88. The system as recited in claim 60, wherein the device processor and the memory are integrated into a single integrated circuit.

89. The system as recited in claim 60, wherein the memory contains a biometric analog of a user.

90. The system as recited in claim 60, wherein the device processor provides binary data to the magnetic field generator after a user has been authenticated using the biometric sensor.

91. The system as recited in claim 60, wherein the device processor deactivates the magnetic field generator after the magnetic field generator has been active for a specified period of time.

92. The system as recited in claim 60, wherein the device processor deactivates the magnetic field generator when the biometric sensor no longer detects the authorized user.

* * * * *

UNIVERSAL SECURE REGISTRY

1. Field of the Invention

5 This invention 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
10 identifications/verifications.

2. Background of the Invention

Dissemination of information regarding various entities, including individuals, in society is conventionally done in a non-centralized fashion, often
15 requiring specialized knowledge of a likely storage location to access the information. This specialized knowledge 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
20 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 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
25 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 patient's primary care physician may not have records from a specialist treating the patient, and none of these physicians may have dental records.
30 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, granting access to information, 5 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 10 employment, one or more credit cards 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 15 that identify the person as owner of an automobile, house, etc., and numerous other identification cards 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 20 to undertake an associated activity. For example, a person is not allowed to drive a car or purchase alcohol without a 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 25 hospitals and other medical facilities will require proof of insurance before rendering medical attention. Carrying these multifarious identification devices can become onerous. 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.

30 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 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
5 some personal information be transmitted to complete a transaction.

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
10 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.

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
20 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
25 general database.

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
30 and protect the individual.

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

5

SUMMARY OF THE 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
10 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
15 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
20 secure registry (USR) system of the type to which this invention relates. For example, in one embodiment, a smart card such as the Secure ID™ 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.

25 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
30 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 persons 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 persons 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.

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 patients medical records, for example x-rays, MRI pictures, dental records, glasses, prescriptions, etc.

Access to the USR system may be by smart card, such as a Secure ID™ 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 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 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 access to ones 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.

BRIEF DESCRIPTION OF THE FIGURES

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;

5 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;

10 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;

15 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;

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

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

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

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

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.

5

DETAILED DESCRIPTION OF THE INVENTION

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 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.

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 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 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

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..

5 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 commercially available operating system, which controls the execution of other computer programs and provides scheduling, debugging, input/output control, 10 accounting, compilation, storage assignment, data management, memory management, communication 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, 15 object-oriented database, unstructured database, or other database. Example relational databases include Oracle 8I 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 20 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 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 25 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 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 30 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 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.

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 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 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 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 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 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 such as the Internet, communications facilitating or relating to transmission of data from/to the USR database 24 or the computer system 10
5 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, for example a
10 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 generator, that communication is with the database and not an imposter.

15 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
20 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
25 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,
30 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.

5 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
10 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
15 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
20 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 using a predetermined algorithm to generate a one-time nonpredictable code which is transmitted to a the computer system 10. The computer system, specifically USR software 18, utilizes the received one-time nonpredictable code to determine if the
25 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 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
30 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 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.

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 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 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 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 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 validation software module may be provided to validate electronic ID devices outside of a firewall segregating the validation information from other user information.

This 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 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, 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. 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 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 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 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.

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 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 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.

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.

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).

5 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 requestors 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
10 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
15 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.

 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
20 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-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
25 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
30 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 one-time 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 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.

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).

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 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 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 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.

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).

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.

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.

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.

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 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 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).

5 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 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
10 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 environment without requiring the user to input address information in connection with every sale.

Fig. 11 illustrates an use of the USR database 24 to deliver mail to a user without
15 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 invention described below, will enable the user to receive parcels without requiring the user to provide the merchant with the address information. Additionally,
20 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 or the duration in which the address will remain valid.

25 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 sending the person one or more parcels.

30 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 Fed Ex to access the address information.

5 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 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
10 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 uses this retrieved information to deliver the package to the user while never supplying the merchant with the user's permanent or temporary
15 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, deliveries to be made on a weekday could be directed to one address and deliveries on a weekend to another address; or
20 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 illustrated in Fig. 12, the user provides a telephone code on the publicly
25 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
10 similar 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
15 car phone during commuting hours, and may wish to have all incoming calls routed to a cell 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
20 be the same, or may be different, there being some advantages to having a single code usable for 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
25 that the right code is selected. The system may similarly be used to provide public keys for use in a public key/private key 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
30 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 system may also be used to perform the encryption. When the recipient receives the message, he deencrypts it using the recipient's private key in standard fashion, including deencrypting 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 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 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, 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 users database could therefore specify that the 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 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.

As can be seen from the above, many of the users of the USR system are
5 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
10 data access 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
15 system to receive updates, 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.

20 Another potential use of the system is to permit a person to be located where only
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
25 response to such an inquiry or to merely be alerted to an inquiry which might involve
them and information on the requester. 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 persons last known address plus school
information, etc. The system will then provide a list of persons who meet the listed
30 criteria from which the person making the inquiry can hopefully find the person they are
looking for.

In the above application and others, when a person is located, the person may request that only the persons address code or general access code (ie 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.

5 Fig. 17 illustrates another embodiment of the invention. As shown in Fig. 17, the 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
10 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, 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
15 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 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
20 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.

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.
25 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.

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.

30 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 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.

5 What is claimed is:

CLAIMS

1. A secure registry system including:
- 5 a database containing selected data on each of a plurality of entities, a code being stored with at least selected portions of said data for at least selected said entities restricting access to said selected portions to entities defined by each said code;
- an identity mechanism which permits each entity to securely identify itself to the system;
- 10 an input mechanism which determines if an identified entity is authorized to enter data into the database, and permits an authorized entity to enter data into the database:
- an access mechanism which permits access requests to be made to said database, each such request including an indication of data requested and at least one of a coded indication of the entity requesting the access and the status of such entity; and
- 15 an entitlement mechanism, including at least in part said identity mechanism, which determines from at least one of provided coded indication of entity and coded indication of entity status whether the entity is entitled to access the requested data, the mechanism granting access to the requested data if the entity is entitled and denying access if the entity is not entitled.
- 20
2. A system as claimed in claim 1 wherein said input mechanism includes a restriction mechanism which permits entities to identify portions of the data relating to them for which there is to be restricted access and to store the appropriate code with each such portion, said restriction mechanism including a change mechanism for permitting
- 25 an entity identified by said identity mechanism to change entities to whom access is granted for at least selected portions of the data for the entity.
3. A system as claimed in claim 2 wherein each entity has a code regimen by which it can be identified by said identity mechanism and a distress code regimen which the
- 30 entity may employ when making at least one of entries and changes in the database to indicate that such is being done under duress; and

a protection mechanism operative in response to receipt of a distress code regimen for initiating appropriate action for the protection of the entity.

4. A system as claimed in claim 1 wherein said entitlement mechanism releases
5 selected portions of data for entities to at least selected classes of data requesters based only on the coded status of such entity.

5. A system as claimed in claim 4 wherein at least selected data requesting entities have a mechanism included in their processors which automatically adds their status code
10 to each data request sent by the entity to the system.

6. A system as claimed in claim 4 wherein at least selected data requesting entities have a mechanism included in their processors which provides a format for requested data; and
15 wherein said system includes a mechanism which accumulates data required to respond to a request in said format and responds to the request with the collected data presented in said format.

7. A system as claimed in claim 1 wherein said coded indication and coded status for
20 an entity are selectively merged into a single coded input to the system for an access requesting entity, the system including a mechanism for determining the coded status and coded indication from the single coded input.

8. A system as claimed in claim 1 wherein an entity requesting data has a
25 mechanism included in their processor which automatically includes with at least selected data requests a coded status indication and a form into which requested information is to be provided; and wherein said entitlement mechanism provides information from the database to which the entity is entitled in the form provided by the entity.

30

9. A system as claimed in claim 1 wherein relevant data is stored in additional databases outside said system;

said system including a retrieval mechanism which, if the entity is entitled to receive such data, retrieves relevant data from a said additional database and provides it to the entity requesting the data in a manner transparent to the entity.

10. A secure registry system for entities, each of which is identified by a multicharacter public code, the system including:

a database from which the public code for each entity may be obtained; and

a processor at a provider of services for entities, said processor including a mechanism for //mapping each received public code to data required by the provider in order to provide the services, (receiving the public code for an entity on whose behalf services are to be provided) and using the corresponding mapped data to perform the services.

11. A system as claimed in claim 10 wherein said provider provides delivery services, the mapped data being an address to which item are to be delivered for the entity, the provider receiving an item to be delivered and a public code for the recipient, and using the public code to obtain the appropriate address for delivery of the item.

12. A system as claimed in claim 10 wherein said provider provides telephone service, the mapped data being a current telephone number for the entity, the provider receiving the public code and connecting the party providing the code to the current telephone number of the entity.

13. A secure registry system including:

a database containing selected data on each of a plurality of entities;

a mechanism by which an organization desiring access to data in said database may gain such access, each said organization having a processor which generates data requests, each such data request including a form in which such data is to be provided; and

a response mechanism which collects data required by said form for a given request, formats the collected data in said form, and sends the formatted data to the organization generating the request.

- 5 14. A secure registry system including:
a database containing biographical data on a plurality of individuals;
a query mechanism by which an entity trying to find an individual can input to the
system a query containing selected biographical data on the individual;
a response mechanism operative in response to a query for providing to the entity
10 selected information on individuals in the system matching the query biological
information; and
a contact mechanism by which the entity making the query can contact a
matching individual only through the system, no contact information being provided to
the entity.

- 15
15. A storage media containing machine readable code which facilitates
communication between a remote machine running the code and a secure registry system
of a type having a database containing selected data on each of a plurality of entities and
restricted access to at least portions of such data, the code causing access requests from
20 the machine to the system to each automatically include at least a status code for the
machine and a format in which data requested is to be presented for response, the system
recognizing the status code to control access to data in the database and using the format
to select the data to be accessed and to control the format in which accessed data is
returned to the machine.

- 25
16. A method for providing a secure registry system including:
a database containing selected data on each of a plurality of entities, a code being
stored with at least selected portions of said data for at least selected said entities
restricting access to said selected portions to entities defined by each said code;
30 permitting each entity to securely identify itself;

determining if an identified entity is authorized to enter data into the database, and permitting an authorized entity to enter data into the database:

5 permitting access requests to be made to said database, each such request including an indication of data requested and at least one of a coded indication of the entity requesting the access and the status of such entity; and

determining from at least one of provided coded indication of entity and coded indication of entity status whether the entity is entitled to access the requested data, granting access to the requested data if the entity is entitled and access being denied if the entity is not entitled.

10

17. A method as claimed in claim 16 wherein said includes a restriction mechanism which permits entities to identify portions of the data relating to them for which there is to be restricted access and to store the appropriate code with each such portion, said restriction mechanism including a change mechanism for permitting an entity identified
15 by said identity mechanism to change entities to whom access is granted for at least selected portions of the data for the entity.

18. A method as claimed in claim 17 wherein each entity has a code regimen by which it can be identified and a distress code regimen which the entity may employ when
20 making at least one of entries and changes in the database to indicate that such is being done under duress; and

a protection mechanism operative in response to receipt of a distress code regimen for initiating appropriate action for the protection of the entity.

25 19. A method as claimed in claim 16 wherein selected portions of data for entities to at least selected classes of data requesters based only on the coded status of such entity are released

20 A method as claimed in claim 16 wherein relevant data is also stored in additional
30 databases outside said system;

said system including a retrieval mechanism which, if the entity is entitled to receive such data, retrieves relevant data from a said additional database and provides it to the entity requesting the data in a manner transparent to the entity.

5 21. A method for providing a secure register for entities, each of which is identified by a multicharacter public code, the system including:

a database from which the public code for each entity may be obtained; and

a provider of servicesprocessor at a provider of services for entities, said processor including a mechanism for receiving the public code for an entity on whose
10 behalf //mapping each received public code to data required by the provider in order to provide the services, (receiving the public code for an entity on whose behalf services are to be provided) and using the corresponding mapped data to perform the services.

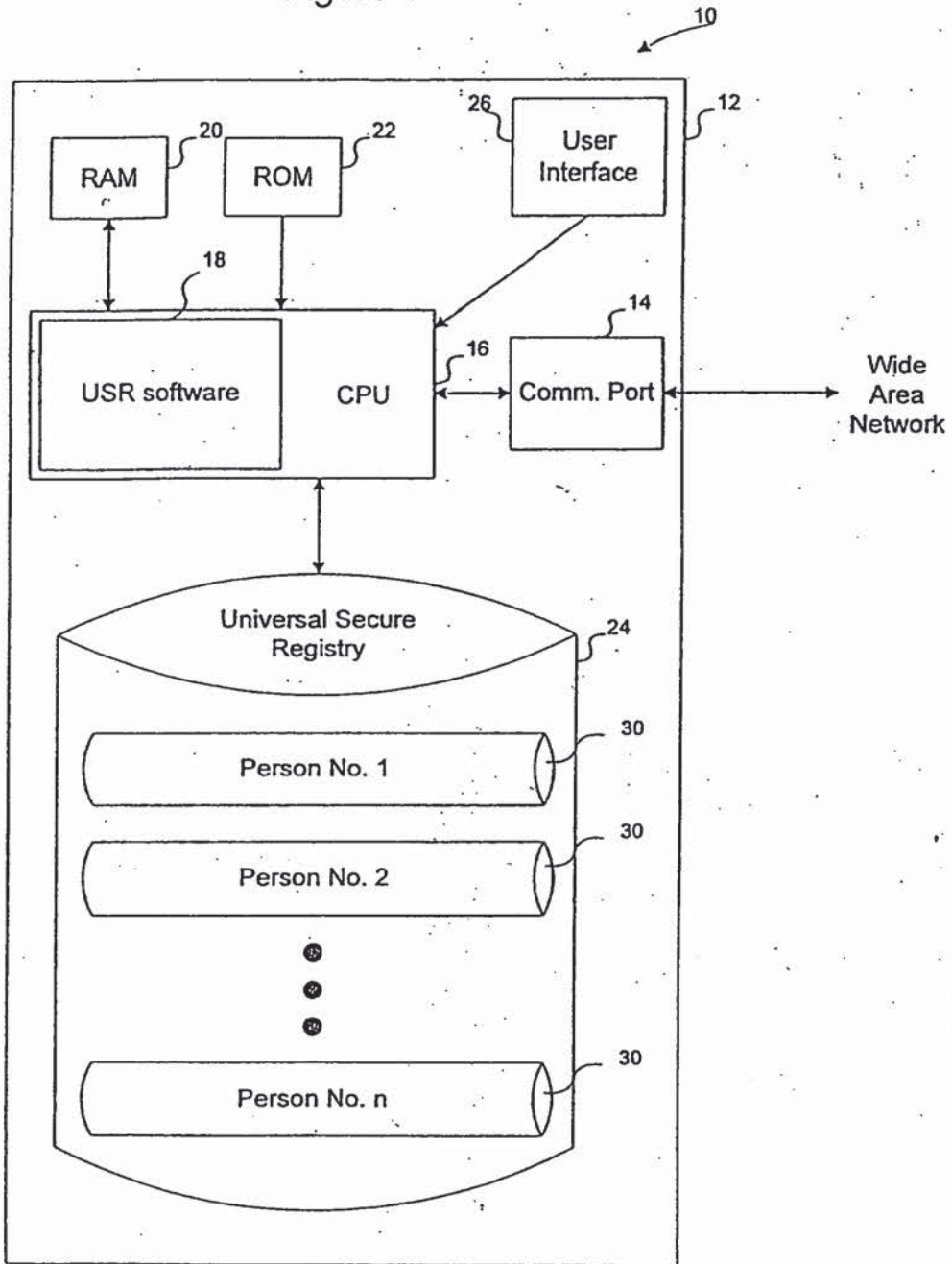
22. A method as claimed in claim 21 wherein said provider provides delivery
15 services, the mapped data being an address to which item are to be delivered for the entity, the provider receiving an item to be delivered and a public code for the recipient, and using the public code to obtain the appropriate address for delivery of the item.

23. A method as claimed in claim 21 wherein said provider provides telephone
20 service, the mapped data being a current telephone number for the entity, the provider receiving the public code and connecting the party providing the code to the current telephone number of the entity.

ABSTRACT

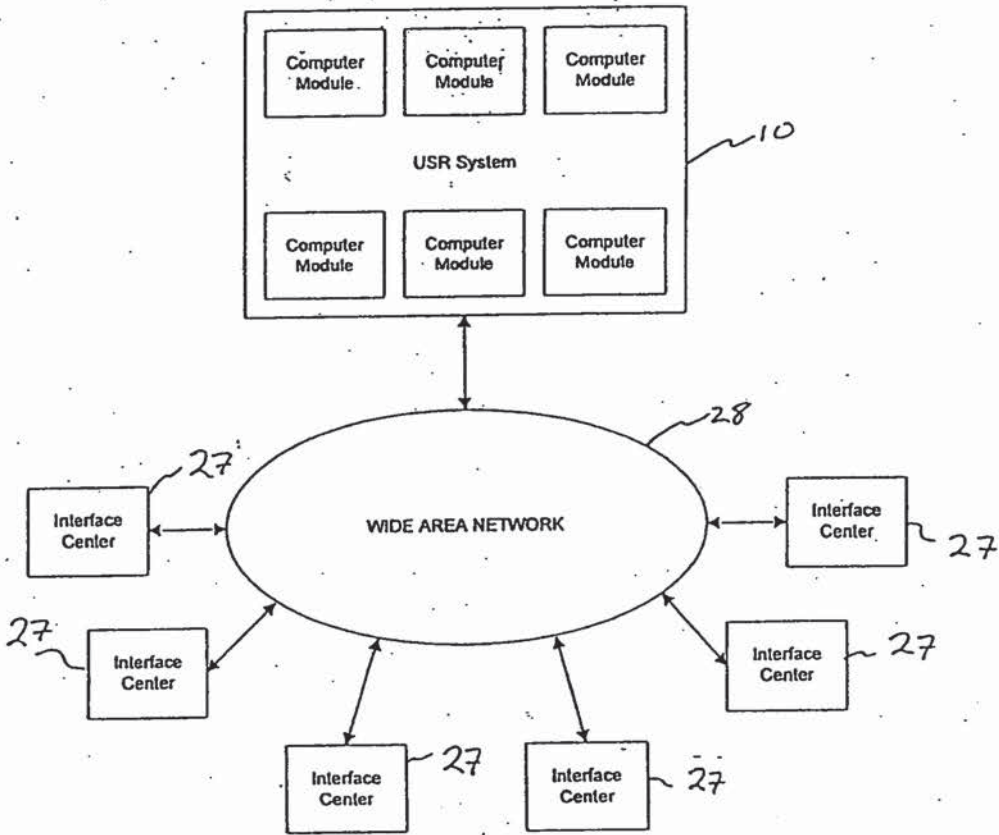
A secure registry system and method for the use thereof are provided which permits secure access to a database containing selected data on a plurality of entities, at least portions of which database has restricted access. Mechanisms are provided for controlling access to restricted access portions of 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 on limited biological data. Organizations utilizing the system may have custom software facilitating their access and use of the system.

Figure 1



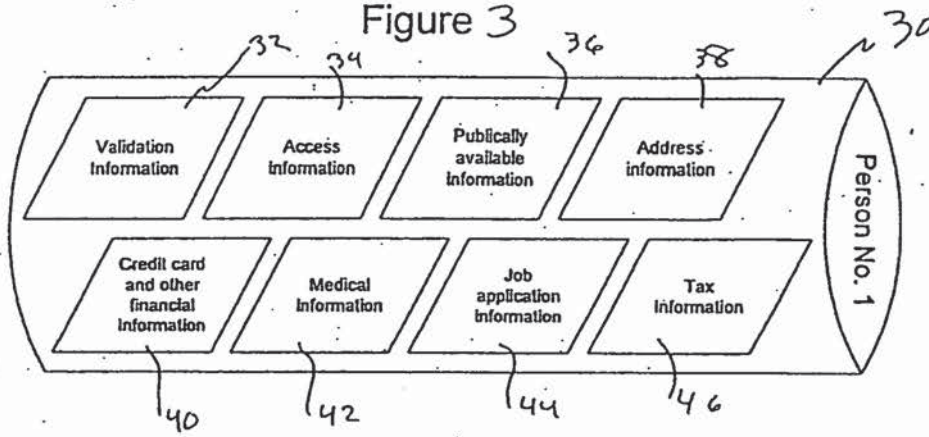
Rest Available Copy

Figure 2



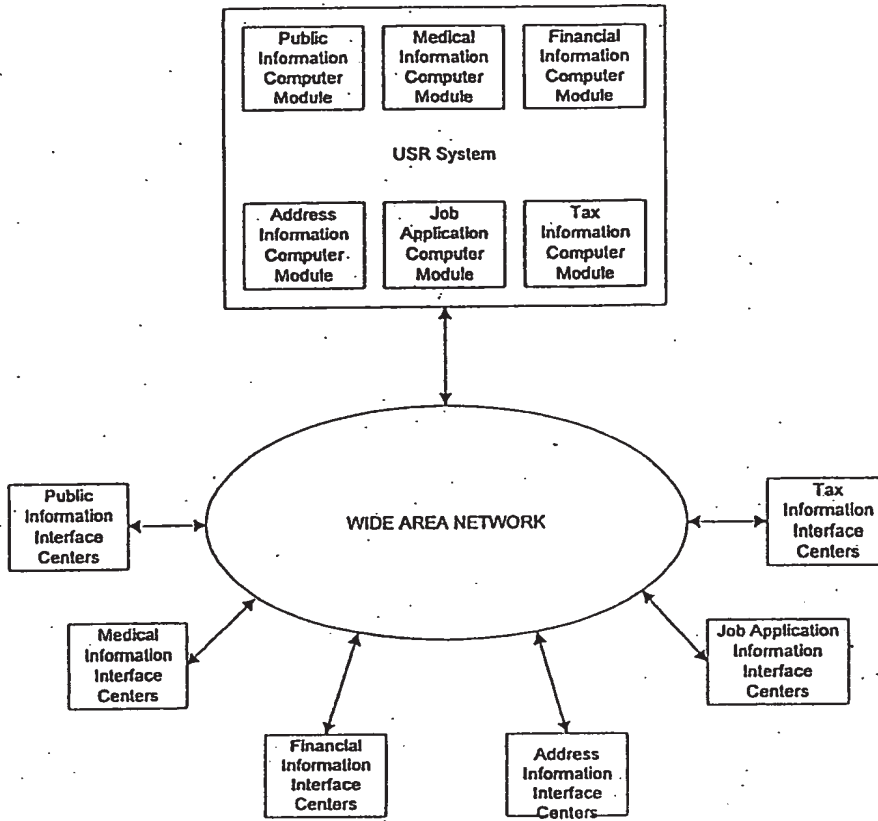
Best Available Copy

Figure 3



Best Available Copy

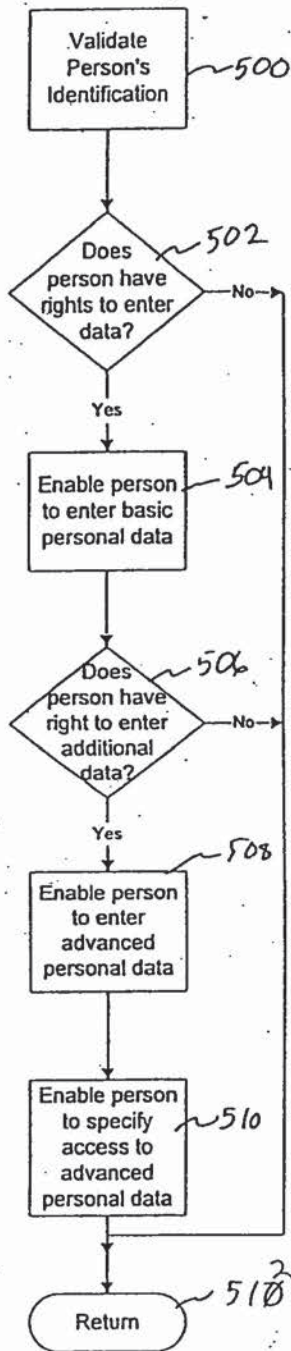
Figure 4



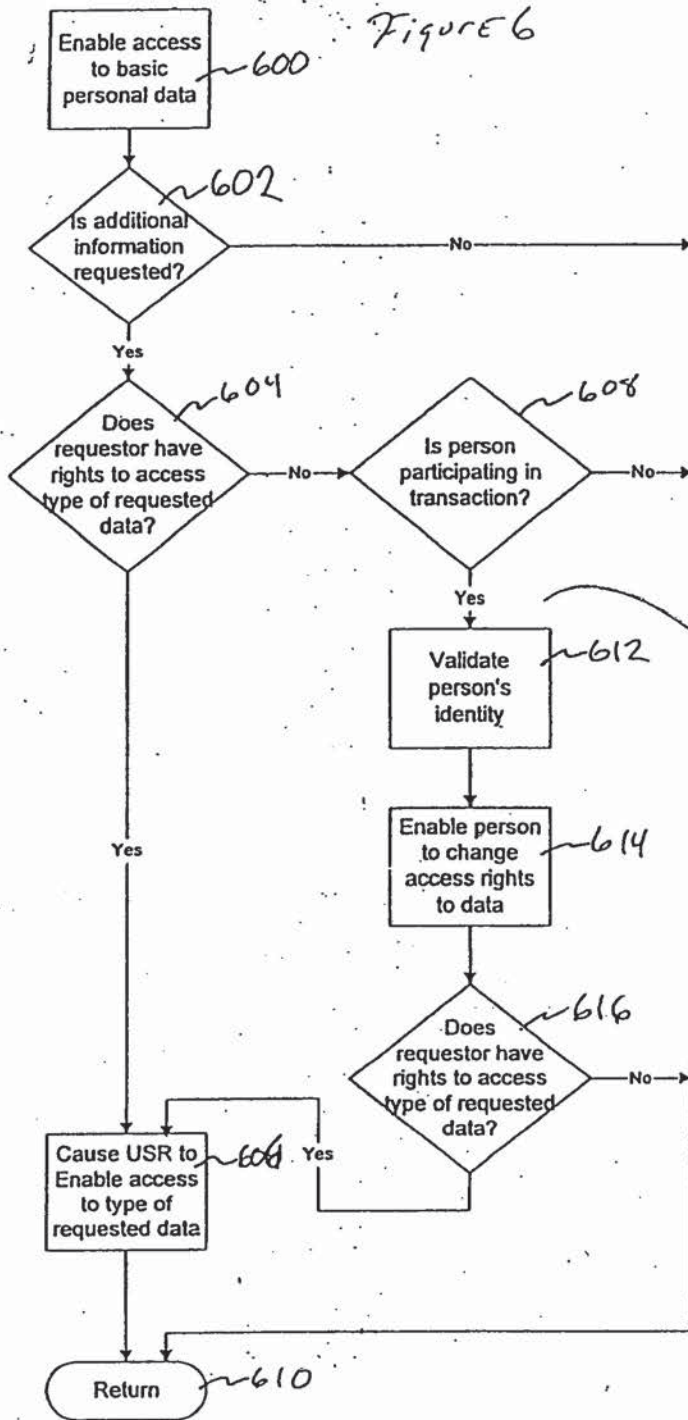
Best Available Copy

Train the Database

FIGURE 5



Rest Available Copy



Best Available Copy

Figure 7

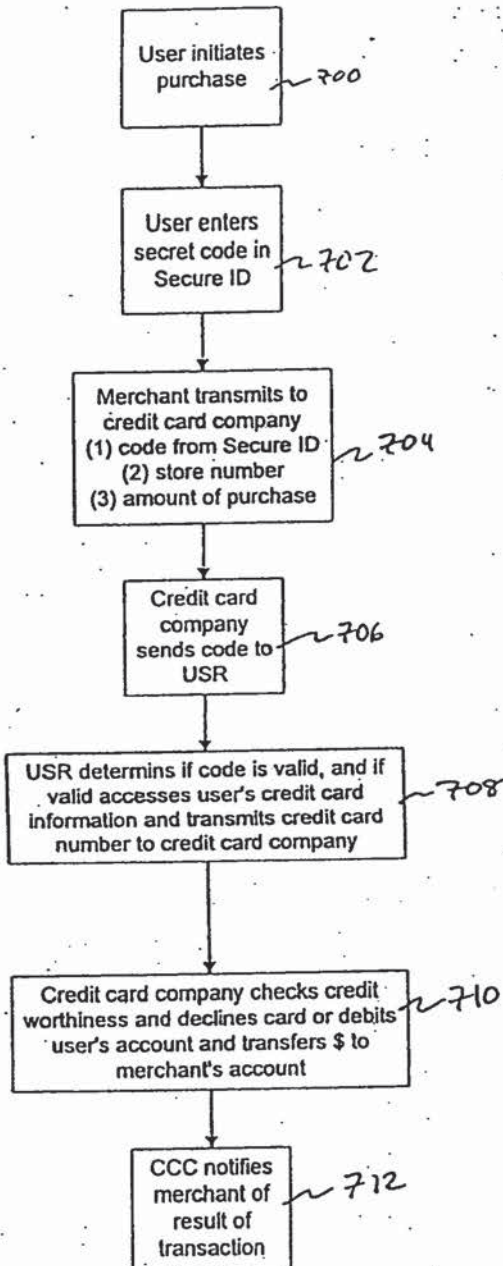
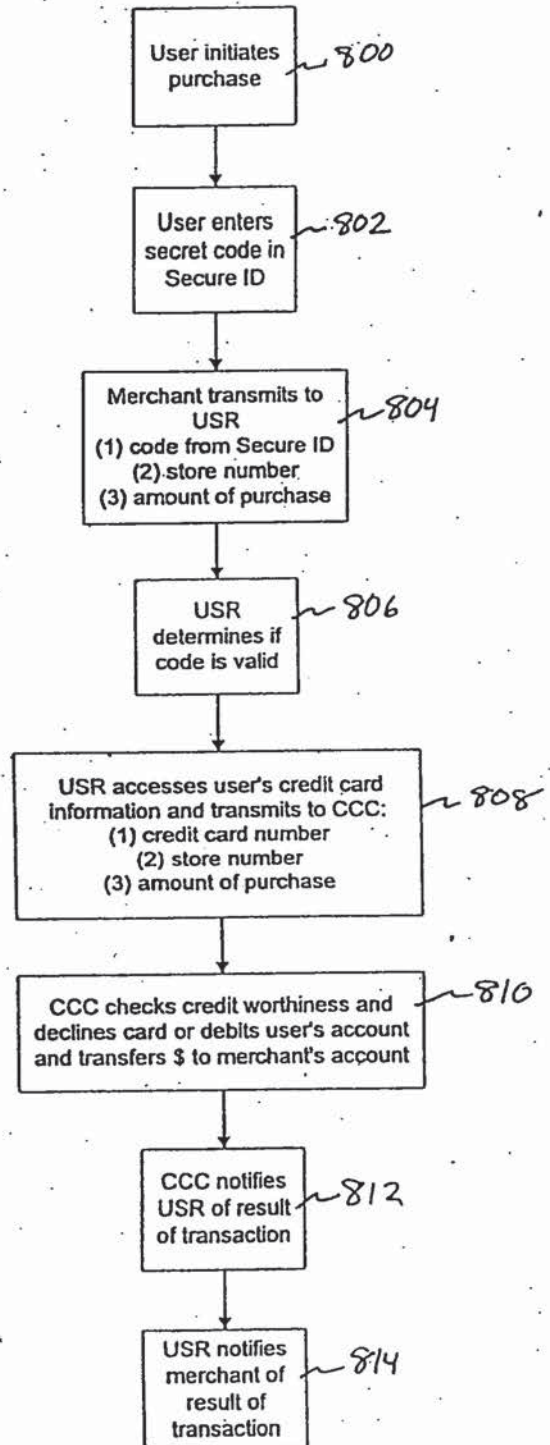
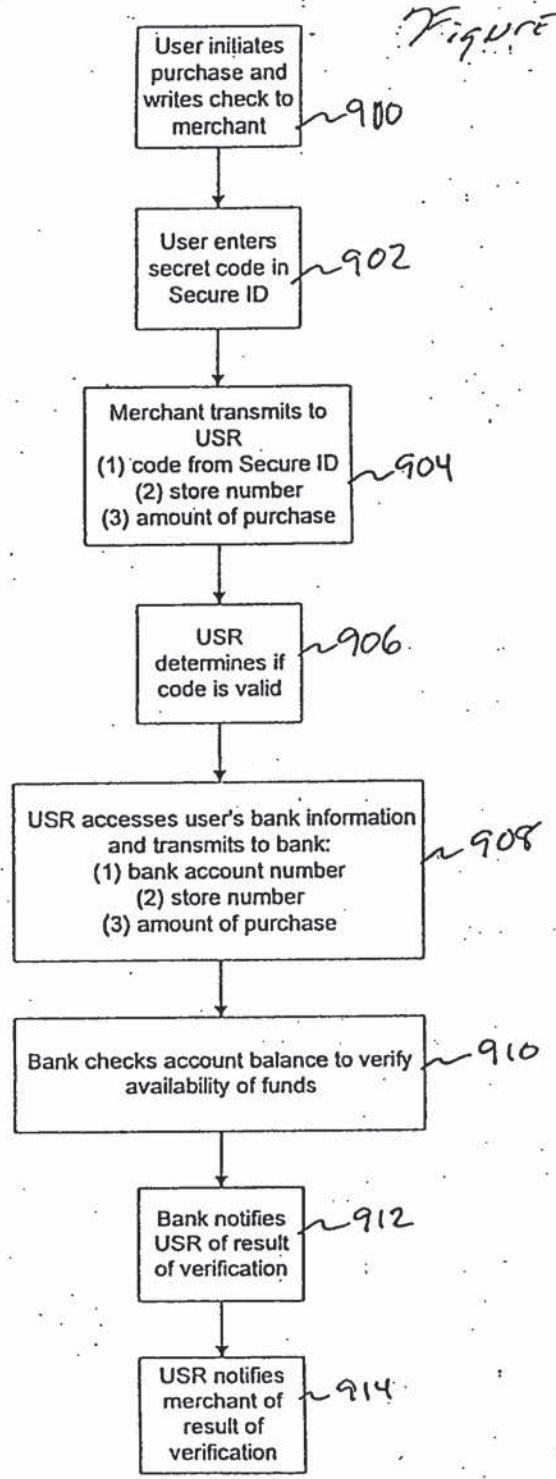


Figure 8



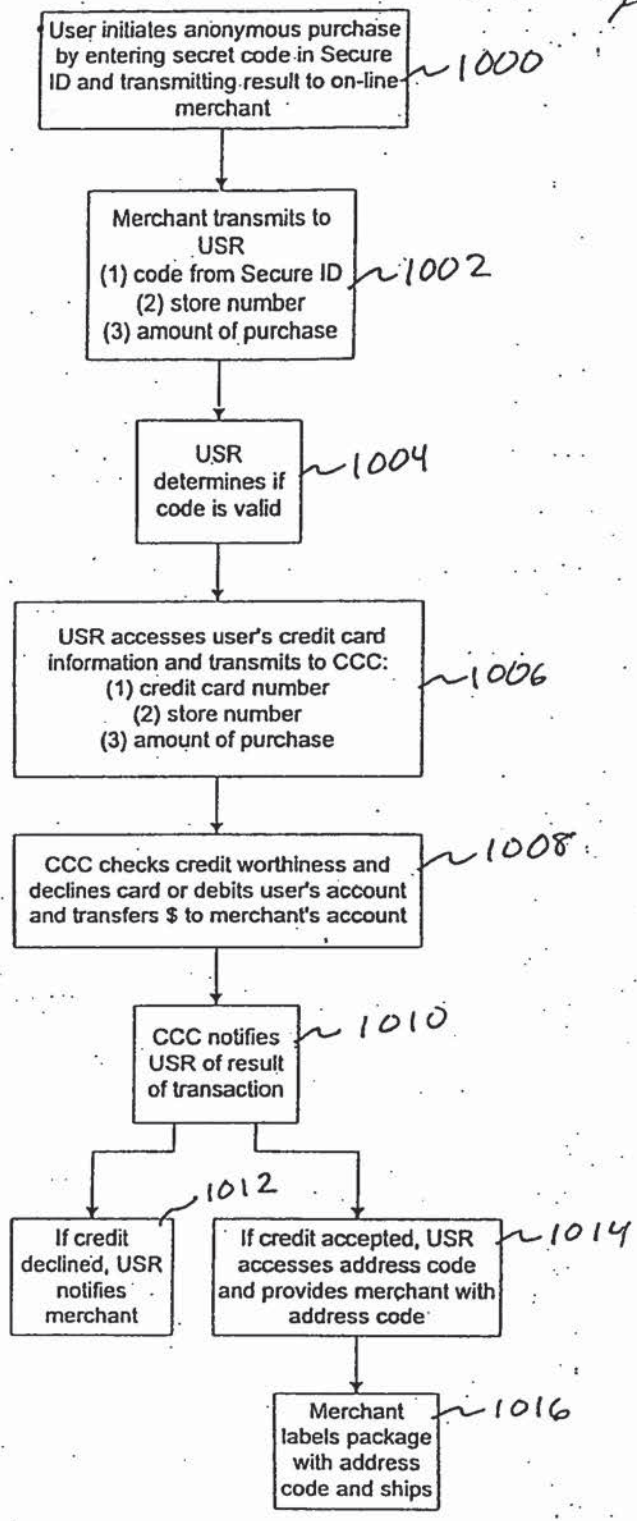
Best Available Copy

Figure 9



Best Available Copy

Figure 10



Best Available Copy

Figure 11

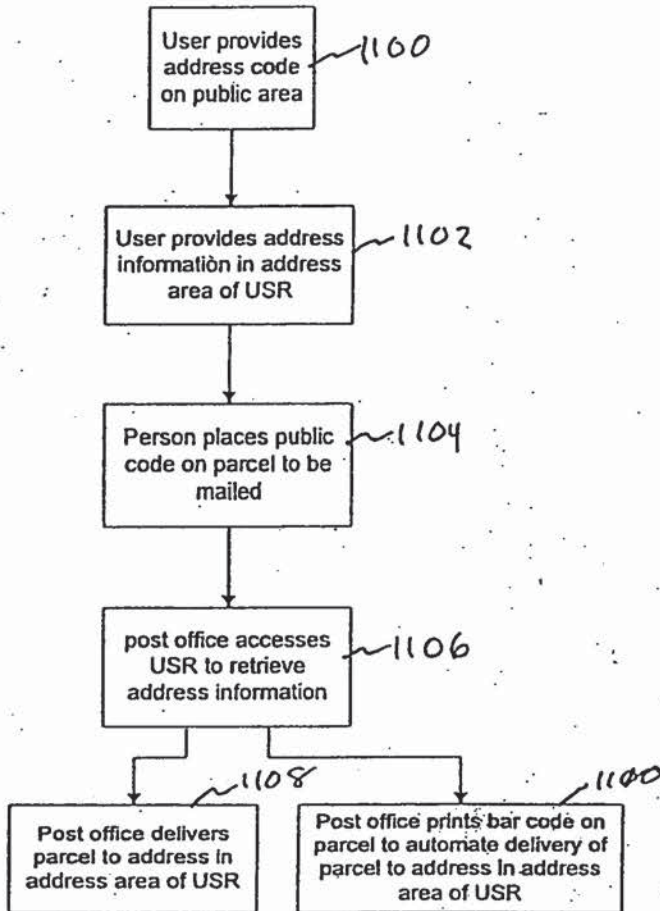


Figure 12

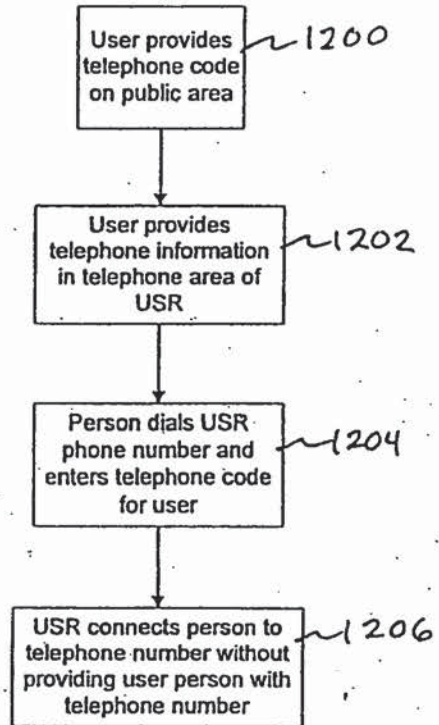


Figure 13

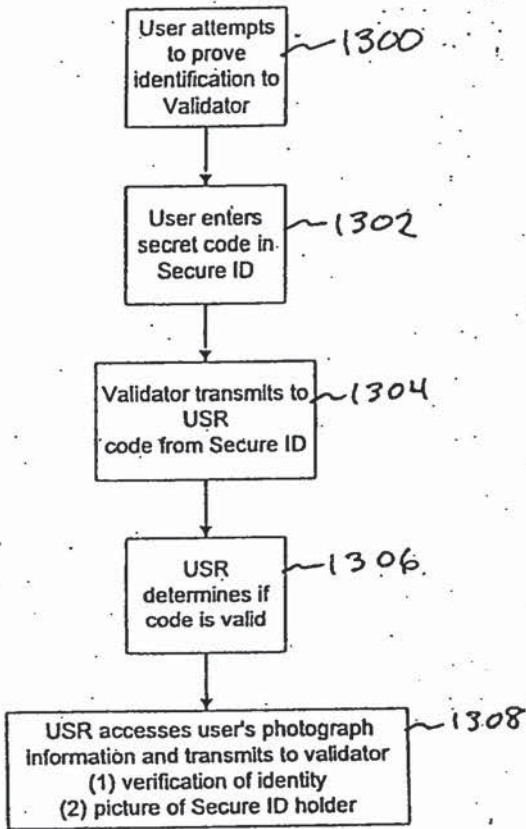


Figure 14

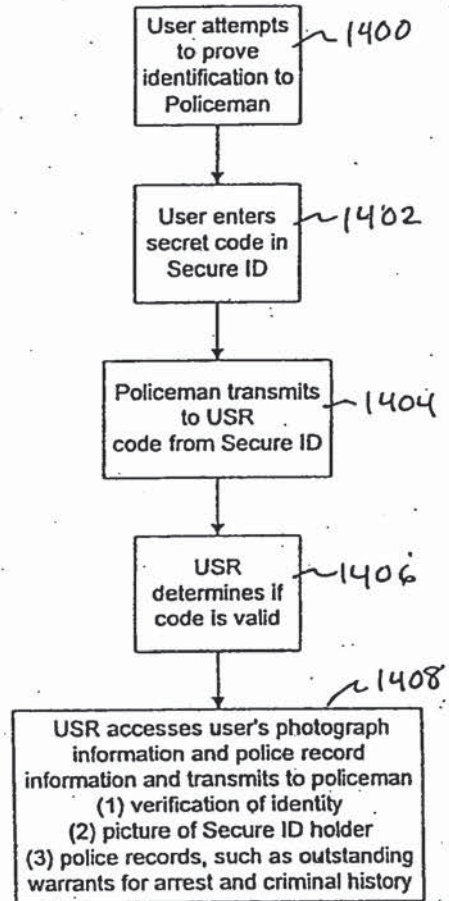


Figure 15

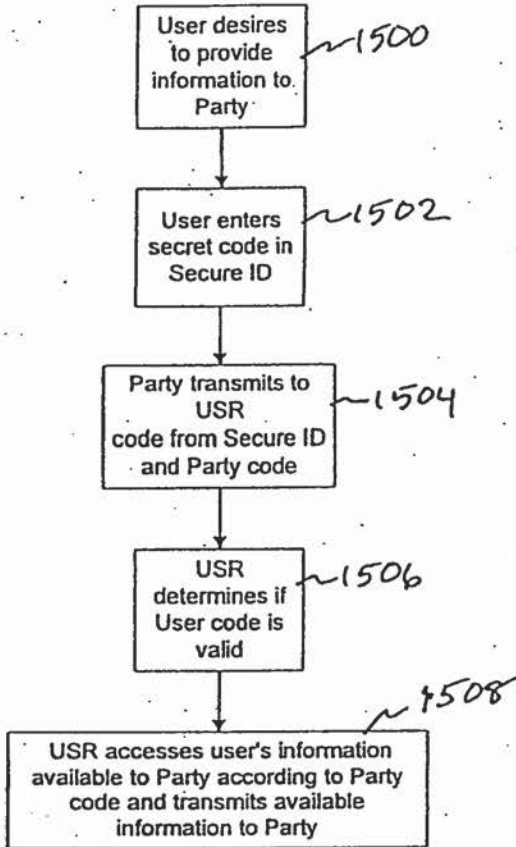
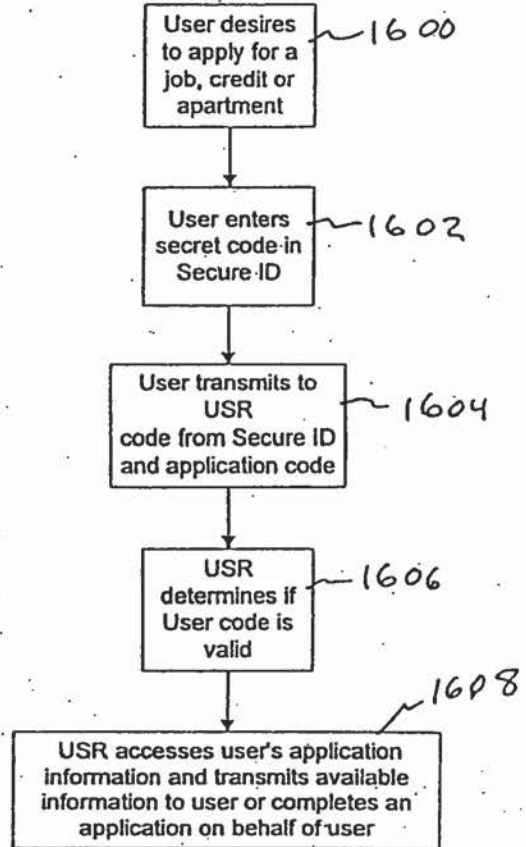
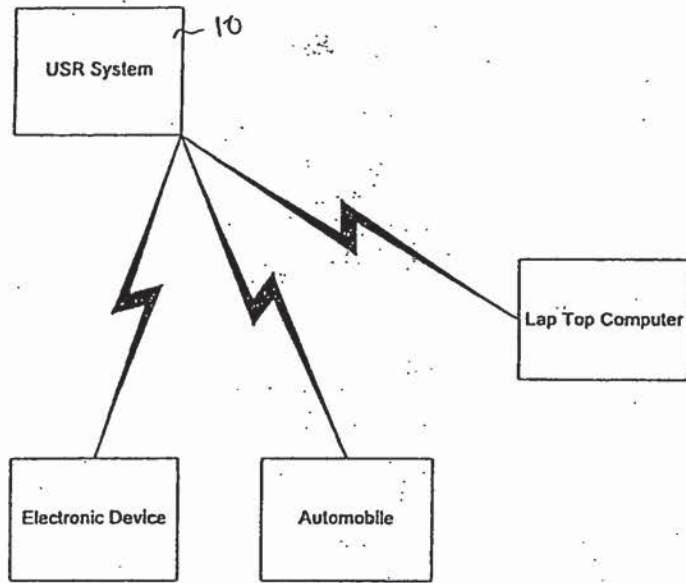


Figure 16



Rest Available Copy

Figure 17



Rest Available Copy