8346394

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

UNITED STATES DEPARTMENT OF COMMERCE

United States Patent and Trademark Office

February 15, 2023

THIS IS TO CERTIFY THAT ANNEXED IS A TRUE COPY FROM THE RECORDS OF THIS OFFICE OF THE FILE WRAPPER AND CONTENTS OF:

APPLICATION NUMBER: ***10/990,296***
FILING DATE: ***November 16, 2004***

UNITED STATES PATENT AND TRADEMARK OFFICE
DEPARTMENT OF COMMERCE

Certified by

Kathi

Performing the Functions and Duties of the
Under Secretary of Commerce
for Intellectual Property
and Director of the United States
Patent and Trademark Office

Attorney Docket: Ryan C-4

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

PATENT APPLICATION TRANSMITTAL

Mail Stop: Patent Application
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Title: MULTI-INTERFACE COMPACT PERSONAL TOKEN APPARATUS AND METHODS OF USE

Inventor(s): Ryan, et al.

Enclosed herewith for filing is:

- PATENT APPLICATION, including:
  - 67 pages of text
  - 4 sheets of drawings
- DECLARATION, not signed

Fee Calculation (Small Entity):

$ 395	Basic Filing Fee
$ 288	32 excess total claims @ $9 each = $288
$ 65	surcharge for late filing fees/signatures
=====	
$ 748	Total Amount Due

This application is being filed "missing parts", without money or signatures.

Please direct all future communications to:

Gerald E. Linden
12925 La Rochelle Cr.
Palm Beach Gardens, FL 33410

Express Mail Certification

I, the undersigned, hereby certify that the enclosed patent application and related papers are being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service under 37 CFR §1.10 on the date indicated below, addressed to Commissioner for Patents, Alexandria, VA 22313.

Express Mail mailing label number - ED 243172992 US

For the Applicant,

Gerald E. Linden 11/16/04

Gerald E. Linden 30,282 date
(561) 694-2094

MULTI-INTERFACE COMPACT PERSONAL TOKEN APPARATUS AND METHODS OF USE

CROSS-REFERENCE TO RELATED APPLICATIONS

This is a non-provisional filing based on USSN 60/520,698 filed 11/17/2003 by Ryan, Comiskey and Knapich.

This is a non-provisional filing based on USSN 60/562,204 filed 4/14/2004 by Comiskey, Finn and Ryan.

This is a non-provisional filing based on USSN 60/602,595 filed 8/18/2004 by Finn.

BACKGROUND OF THE INVENTION

1. Technical Field

This invention relates generally to smart card technology.

2. Related Art

A smart card resembles a credit card in size and shape. (See ISO 7810). The inside of a smart card usually contains an embedded 8-bit microprocessor. The microprocessor is under a gold contact pad on one side of the card. Smarts cards may typically have 1 kilobyte of RAM, 24 kilobytes of ROM, 16 kilobytes of programmable ROM, and an 8-bit microprocessor running at 5 MHz. The smart card uses a serial interface and receives its power from external sources like a card reader. The processor uses a limited instruction set for applications such as cryptography. The most common smart card applications are:

- Credit cards
- Electronic cash
- Computer security systems
- Wireless communication
- Loyalty systems (like frequent flyer points)

- Banking
- Satellite TV
- Government identification

Smart cards can be used with a smart-card reader attachment to a personal computer to authenticate a user. (However, these readers are relatively costly, and have not been well accepted by users.) Web browsers also can use smart card technology to supplement Secure Sockets Layer (SSL) for improved security of Internet transactions. The American Express Online Wallet shows how online purchases work using a smart card and a PC equipped with a smart-card reader. Smart-card readers can also be found in vending machines.

There are three basic types of smart cards: contact chip, contactless and dual interface (DI) cards.

A contact smart card (or contact chip card) is a plastic card about the size of a credit card that has an embedded integrated circuit (IC) chip to store data. This data is associated with either value or information or both and is stored and processed within the card's chip, either a memory or microprocessor device.

The predominant contact smart cards in consumer use are telephone cards as a stored value tool for pay phones and bank cards for electronic cash payments. Contact smart cards require the placement of the card in a terminal or automatic teller machine for authentication and data transaction. By inserting the contact smart card into the terminal, mechanical and electrical contact is made with the embedded chip module.

Contactless smart cards have an embedded antenna connected to a microchip, enabling the card to pick up and respond to radio waves. The energy required for the smart card to manipulate and transmit data is derived from the electromagnetic field generated by a reader. Contactless smart cards do not require direct contact with the reader because they employ the passive transponder technology of Radio Frequency Identification (RFID). By just waving the card near the reader, secure identification, electronic payment transaction and authentication are completed in milliseconds.

Contactless chip card technology is based on two standards: ISO/IEC 14443 Type A and Type B (for proximity cards), and ISO/IEC 15693 (for vicinity cards). Cards that comply with these standards operate at the 13.56 MHz frequency. ISO/IEC 14443 products have a range of up to 10 cm (centimeters), while ISO/IEC 15693 products can operate at a range between 50 and 70 cm.

Dual interface (DI) cards, sometimes called combination chip cards, are microprocessor multi-function cards that incorporate both the functions of a contact chip card and a contactless card. Within the smart card is a microprocessor or micro-controller chip with radio frequency identification (RFID) capability that manages the memory allocation and file access. The on-board memory is shared and can be accessed either in contact or contactless mode.

This type of chip is similar to those found inside all personal computers and when implanted in a smart card, manages data in organised file structures, via a card operating system. This capability permits different and multiple functions and/or different applications to reside on the card.

A dual interface (DI) card is ideal for single and multi-application markets ranging from micro-payment (convenient alternative to low value cash transaction) to e-commerce and from ticketing in mass transit to secure identification for cross border control. Originally, such cards were intended to be used in conjunction with a reader connected to a PC for downloading tickets, tokens, or electronic money via the contact interface and used in contactless mode in the application for physical access or proximity payment

Passive radio frequency identification (RFID) devices derive their energy from the electromagnetic field radiated from the reader. Because of international power transmission restrictions at the frequencies of 125 KHz and 13,56 MHz, the contactless integrated circuits are generally low voltage and low power devices. Read/Write circuits use low voltage EEPROM and low power analogue cells. The read/write memory capacity in transponders, contact smart cards, contactless memory based smart cards, dual interface smart cards (contact & contactless) and multi-interface micro-controllers is generally limited to approximately 64 kilobytes.

The dual interface (DI) smart cards typically have an 8, 16 or 32 bit microprocessor controller, operate at a low voltage of 1.8V-5V and run at an internal frequency of 5 or 15 MHz. The open platform architecture includes memory management, non volatile memory, contactless interfaces and security features such as Advanced Crypto Engine (ACE) 1100 bit, triple DES encryption and RSA.

High performance crypto controllers with multiple interfaces such as USB, ISO 14443 Type A, B, Felica have been developed for multi-functional smart cards in applications such as security access, healthcare, electronic purse, banking etc.

The main focus of the smart card industry has been on secure card applications, where large memory capacity is not of paramount importance, and/or where pertinent information and application software is stored at a centralised server location.

Another market area that has been evolving in recent years is memory, particularly for computing devices which are capable of interacting with large amounts of data and implementing sophisticated functionality, such as laptops, cameras, mobile phones, PDAs, MP3 players, and the like.

The main focus of the flash drive industry is on high density memory (using NAND flash memory cells) and current USB key chain products from the market leaders incorporate an 8-Gigabyte flash memory chip, managed by a 32 bit micro-controller.

These large capacity, personal, portable storage devices are for decentralised applications to transport confidential business documents, multimedia files, photos, music files, address book, favorite web sites, games, etc.

Apart from using USB tokens for file storage, they are also used for desktop settings, screen lock, network login & access control, log book, user authentication (storing digital signatures, certificates, key sets, finger-based biometric templates, usernames and passwords), digital content and transaction security as well as enterprise and Internet security.

A USB token can also be used to download emails, remotely access a PC or to open a customised browser that allows the user to surf the Web with total privacy.

Recent developments in USB flash memory drives have resulted in CDROM-like auto-run devices that automatically execute a file when the USB token is inserted into a PC. The read-only and auto-run contents are installed during the manufacturing process. Examples of auto-run contents include opening a website, running a demo application, showing a presentation, making a product pitch, providing customers with discount coupons etc.

Related Patents and/or Publications

US Patent Publication No. 2003/0028797 discloses integrated USB connector for personal token. A personal key having an inexpensive and robust integrated USB connector is disclosed. The apparatus comprises a circuit board having a processor and a plurality of conductive traces communicatively coupling the processor to a peripheral portion of the circuit board. The plurality of conductive traces includes, for example, a power trace, a ground trace, and at least two signal traces. The apparatus also comprises a first housing, having an aperture configured to accept the periphery of the circuit board therethrough, thereby presenting the plurality of conductive traces exterior to the aperture. The apparatus also comprises a shell, surrounding the plurality of conductive traces, the shell including at least one locking member interfacing with the first housing.

US Patent Publication No. 2002/0011516 discloses smart card virtual hub. A smart card virtual hub combines a ISO7816 compliant smart card reader interface with a USB hub that provides one or more attachment points for connection of devices to the USB bus, thereby interfacing such devices to the host computer. The hub in the presently preferred embodiment of the invention provides one port to which one USB functional device, such as a keyboard, may be attached. The attached keyboard shares a common USB bus bandwidth with the internal embedded smart card reader through a host-scheduled, token-based communication protocol that is handled by the USB driver and the device driver.

US Patent Publication No. 2003/0102380 discloses a memory card and a method for operating a memory card, the memory card comprising: a memory mass storage; a first data interface with a contacting interface and a high data transfer rate; a second data interface with a contact-less interface. In a preferred embodiment, a memory card controller is included for selecting a first data line from said first data interface or a second data line from said second data interface to communicate with said memory mass storage based on a criteria.

US Patent Publication No. 2003/0087601 discloses an apparatus, system and method for communicating between a personal device and a host computer. The apparatus comprises means for wireless communication, for enabling communication with a personal device (which also comprises means for wireless communication) and means for wired communication for enabling communication with the host computer (which also comprises means for wired communication). A controller installed within the apparatus, controls the data transfer between the wireless and wired communication interfaces of the apparatus. The controller may perform additional computing operations, such as security related operations (e.g. digitally signing a document, ciphering, and so forth). The apparatus may further comprise a smartcard chip, for securely storing information, and also for performing the additional computing operations. Implementations of the invention can be carried out in order to functionally connect a personal device, such as PDA, mobile phone, and so forth, to a host computer, or with an application executed on the host computer. The apparatus may be used to for security implementations, e.g. provision of PINs, keys, passwords, digitally signing of documents, and so forth. The personal device may also be used as input means for the apparatus, thereby enabling a large number of implementations, including applications with relevancy to cellular telephony.

WIPO Publication No. WO 01/96990 discloses USB-Compliant Personal Key Using a Smartcard Processor and a Smartcard Reader Emulator. A compact, self-contained, personal key is disclosed. The personal key comprises a USB-compliant interface releaseably coupleable to a host processing device operating under command of an operating system; a smartcard processor having a smartcard processor-compliant interface of communicating according to a smartcard input and output protocol; and an interface processor, communicatively coupled to the USB-compliant interface and to the smartcard processor-compliant interface, the interface processor implementing a translation module for interpreting USB-compliant messages into smartcard processor-compliant messages and for interpreting smartcard processor-compliant messages into USB-compliant messages.

WIPO Publication No. WO 00/42491 discloses USB-Compliant Personal Key with Integral Input and Output Devices. A compact, self-contained, personal key is disclosed. The personal key comprises a USB-compliant interface (206) releasably coupleable to a host processing device (102); a memory (214); and a processor (212). The processor (212) provides the host processing device (102) conditional access to data storable in the memory (214) as well as the functionality required to manage files stored in the personal key and for performing computations based on the data in the files. In one embodiment, the personal key also comprises an integral user input device (218) and an integral user output device (222). The input and output devices (218, 222) communicate with the processor (212) by communication paths (220, 222) which are independent from the USB-compliant interface (206), and thus allow the user to communicate with the processor (212) without manifesting any private information external to the personal key.

WIPO Publication No. WO 01/39102 discloses PORTABLE READER FOR SMART CARDS. A portable reader (1) for smart cards (7) is described that comprises: a support body (3) containing at least one slot (5) for inserting and reading a smart card (7); interface means (9) connected to the support body (3); interface means (9) connected to the support body (3); means (13) for keeping and aligning the smart card (7); and a managing microprocessor contained inside the support body (3) and connected to the interface means (9) and the reading means for smart cards (7).

US Patent No. 5,761,648 discloses interactive marketing network and process using electronic certificates. A data processing system issuing electronic certificates through "online" networks of personal computers, televisions, or other devices with video monitors or telephones. Each electronic certificate includes transaction data and identification data, and can be printed out on a printing device linked to a consumer's personal input device, or electronically stored in a designated data base until a specified expiration date. The certificate can be used for various purposes, including use as a coupon for a discounted price on a product or service, proof of a gift or award, proof of reservation, or proof of payment. Consumers access the data processing system online, browse among their choices, and make their selections. The data processing system provides reports on the selected certificates and their use following selection. Certificate issuers also have online access to the data processing system and can create or revise offers, and provide various instructions pertaining to the certificates, including limitations as to the number of certificates to be issued in total and to each individual consumer. (see also www.coolsavings.com)

U.S. Patent No. 6,694,399 discloses method and device for universal serial bus smart card traffic signalling. A method and device are disclosed for detecting successful transfers between a Universal Serial Bus (USB) port and a USB smart card and generating a signal that provides an indication of the USB transaction activity. This USB transaction activity signal is modulated according to the USB transaction activity and drives a Light Emitting Diode (LED) in a preferred embodiment of the invention. A counter internal to the USB smart card scales the transaction activity signal such that it is perceptible to the user. Because the current through the LED depends upon the USB transaction activity, the brightness of the LED varies according to the USB transaction activity. The LED may be driven from a current mirror sink or source, or a current switch sink or source.

GLOSSARY, DEFINITIONS, BACKGROUND

The following terms may be used throughout the descriptions presented herein and should generally be given the following meaning unless contradicted or elaborated upon by other descriptions set forth herein. Many of the definitions below were taken from http://www.webopedia.com. Some of the terms set forth below may be registered trademarks (®).

BIOS Short (e.g., acronym or abbreviation) for " basic input/output" system. BIOS is the built-in software that determines what a computer can do without accessing programs from a disk. On PCs, the BIOS contains all the code required to control the keyboard, display screen, disk drives, serial communications, and a number of miscellaneous functions.

Bluetooth A wireless technology developed by Ericsson, Intel, Nokia and Toshiba that specifies how mobile phones, computers and PDAs interconnect with each other, with computers, and with office or home phones. The technology enables data connections between electronic devices in the 2.4 GHz range at 720 Kbps (kilo bits per second) within a 30-foot range. Bluetooth uses low-power radio frequencies to transfer information wirelessly between similarly equipped devices.

CDMA Short for "Code-Division Multiple Access". CDMA is a digital cellular technology that uses spread-spectrum techniques. Unlike competing systems, such as GSM, that use TDMA, CDMA does not assign a specific frequency to each user. Instead, every channel uses the full available spectrum. Individual conversations are encoded with a pseudo-random digital sequence.

cell phone Also referred to as "mobile phone" or "handset". A cell phone today is a mobile communication device used not only for making calls, but it is lately used as media device, transaction device, data storage device using SD or MMC cards for that. So called smart cellular phones are also Internet enabled devices allowing the user to connect to and browse the world wide web, send and receive email, and some also incorporate the functionality of a PDA.

cf. Short for the Latin "confer". As may be used herein, "compare".

computer A programmable machine. The two principal characteristics of a computer are:

- It responds to a specific set of instructions in a well-defined manner.
- It can execute a prerecorded list of instructions (a program).

Modern computers are electronic and digital. The actual machinery - wires, transistors, and circuits - is called hardware; the instructions and data are called software.

DNS Short for "Domain Name System" (or Service or Server). DNS is an Internet service that translates domain names into IP addresses. Because domain names are alphabetic, they're easier to remember. The Internet however, is really based on IP addresses. Every time you use a domain name, therefore, a DNS service must translate the name into the corresponding IP address. For example, the domain name www.example.com might translate to 198.105.232.4. The DNS system is, in fact, its own network. If one DNS server doesn't know how to translate a particular domain name, it asks another one, and so on, until the correct IP address is returned.

DSL Short for "Digital Subscriber Line". DSL technologies use sophisticated modulation schemes to pack data onto copper wires. They are sometimes referred to as last-mile technologies because they are used only for connections from a telephone switching station to a home or office, not between switching stations. The two main categories of DSL are ADSL (asymmetric DSL) and SDSL (symmetric DSL). ADSL supports data rates of from 1.5 to 9 Mbps (million bits per second) when receiving data (known as the downstream rate) and from 16 to 640 Kbps when sending data (known as the upstream rate). Two other types of DSL technologies are High-data-rate DSL (HDSL) and Very high DSL (VDSL).

EEPROM Short for "electrically erasable programmable read-only memory". EEPROM is a special type of PROM that can be erased by exposing it to an electrical charge. Like other types of PROM, EEPROM retains its contents even when the power is turned off. EEPROM is similar to flash memory (sometimes called flash EEPROM). The principal difference is that EEPROM requires data to be written or erased one byte at a time whereas flash memory allows data to be written or erased in blocks. This makes flash memory faster.

e.g. Short for the Latin "exempli gratia". Also "eg" (without periods). As may be used herein, means "for example".

etc. Short for the Latin "et cetera". As may be used herein, means "and so forth", or "and so on", or "and other similar things (devices, process, as may be appropriate to the circumstances)".

Ethernet A local-area network (LAN) architecture developed by Xerox Corporation in cooperation with DEC and Intel in 1976. Ethernet uses a bus or star topology and supports data transfer rates of 10 Mbps. The Ethernet specification served as the basis for the IEEE 802.3 standard, which specifies the physical and lower software layers. Ethernet uses the CSMA/CD access method to handle simultaneous demands. It is one of the most widely implemented LAN standards. A newer version of Ethernet, called 100Base-T (or Fast Ethernet), supports data transfer rates of 100 Mbps. And the newest version, Gigabit Ethernet supports data rates of 1 gigabit (1,000 megabits) per second.

expansion card A stamp-sized add-on memory that a user inserts into an expansion slot of a device such as a PDA. Expansion cards can contain applications, songs, videos, pictures, and other information in a digital format. They also come in three 'flavors': MultiMediaCard™ (MMC), SD (Secure Digital) card and SDIO (Secure Digital Input/Output) card. Mini SD Card

Firewall A system designed to prevent unauthorized access to or from a private network. Firewalls can be implemented in both hardware and software, or a combination of both. Firewalls are frequently used to prevent unauthorized Internet users from accessing private networks connected to the Internet, especially intranets. All messages entering or leaving the intranet pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. There are several types of firewall techniques:

- Packet filter: Looks at each packet entering or leaving the network and accepts or rejects it based on user-defined rules. Packet filtering is fairly effective and transparent to users, but it is difficult to configure. In addition, it is susceptible to IP spoofing.

- Application gateway: Applies security mechanisms to specific applications, such as FTP and Telnet servers. This is very effective, but can impose a performance degradation.

- Circuit-level gateway: Applies security mechanisms when a TCP or UDP connection is established. Once the connection has been made, packets can flow between the hosts without further checking.

-Proxy server: Intercepts all messages entering and leaving the network. The proxy server effectively hides the true network addresses.

In practice, many firewalls use two or more of these techniques in concert. A firewall is considered a first line of defense in protecting private information. For greater security, data can be encrypted.

flash memory A special type of EEPROM that can be erased and reprogrammed in blocks instead of one byte at a time. Many modern PCs have their BIOS stored on a flash memory chip so that it can easily be updated if necessary. Such a BIOS is sometimes called a flash BIOS. Flash memory is also popular in modems because it enables the modem manufacturer to support new protocols as they become standardized.

GSM/GPRS Short for "Global System for Mobile Communications"/"General Packet Radio Service". A type of mobile phone network used throughout most of the world. GPRS enabled networks offer 'always-on', higher capacity, Internet-based content and packet-based data services. This enables services such as color Internet browsing, email on the move, powerful visual communications, multimedia messages and location-based services. Used by AT&T, Cingular Wireless and T-Mobile (and others) in the USA and Rogers Wireless and Fido in Canada. GSM 11.11 is a specification for Global System for Mobile communications.

handheld A portable electronic device that fits in a hand or pocket and functions as a personal organizer, but can also contain other applications that enable you to listen to music, view photos, read eBooks, play games, view and edit documents, and more. Also commonly called a Personal Digital Assistant (PDA).

i.e. Short for the Latin "id est". As may be used herein, "that is".

IEC Short for "International Electrotechnical Commission".

IEEE Short for "Institute of Electrical and Electronics Engineers". The IEEE is best known for developing standards for the computer and electronics industry.

IEEE 812.11 The IEEE standard for wireless Local Area Networks (LANs). It uses three different physical layers, 802.11a, 802.11b and 802.11g.

IEEE 1394 IEEE 1394 (also known as FireWire® and iLINK™) is a high-bandwidth isochronous (real-time) interface for computers, peripherals, and consumer electronics products such as camcorders, VCRs, printers, PCs, TVs, and digital cameras. With IEEE 1394-compatible products and systems, users can transfer video or still images from a camera or camcorder to a printer, PC, or television (TV), with no image degradation.

Internet A global network connecting millions of computers for the exchange of data, news and opinions. Unlike online services, which are centrally controlled, the Internet is decentralized by design. Each Internet computer, called a host, is independent. Its operators can choose which Internet services to use and which local services to make available to the global Internet community. Remarkably, this anarchy by design works exceedingly well. There are a variety of ways to access the Internet. Most online services, such as America Online, offer access to some Internet services. It is also possible to gain access through a commercial Internet Service Provider (ISP).

I/O Short for "Input/Output".

ISO Short for "International Organization for Standardization." (Note that ISO is not an acronym; instead, the name derives from the Greek word iso, which means equal.)

ISO 14443 ISO 14443 RFID cards; contactless proximity cards operating at 13.56 MHz in up to 5 inches distance. ISO 14443 defines the contactless interface smart card technical specification.

ISO 7810 Defines the size and shape of cards. All credit cards and debit cards, and most ID are the same shape and size, as specified by the ISO 7810 standard. Smart cards follow specifications set out in ISO 7816, and contactless smart cards follow the ISO 14443 specification.

ISO 7816 Regarding smart card, ISO7816 defines specification of contact interface IC chip and IC card.

ISO 15693

ISO standard for contactless integrated circuits, such as used in RF-ID tags. ISO 15693 RFID cards; contactless vicinity cards operating at 13.56 MHz in up to 50 inches distance. (ISO 15693 is typically not used for financial transactions because of its relatively long range as compared with ISO 14443.)

LAN

Short for "Local Area Network". A computer network that spans a relatively small area. Most LANs are confined to a single building or group of buildings. However, one LAN can be connected to other LANs over any distance via telephone lines and radio waves. A system of LANs connected in this way is called a wide-area network (WAN).

memory

Storage for applications, photos, videos and other data in a device, measured in megabytes (MB). The more memory, the more applications, photos, videos and other data a device can store. Four types of memory are available:

1) fixed built-in random access memory (RAM) included with the device,

2) add-on memory, sold separately, in the form of expansion cards of various capacities,

3) fixed built-in read-only memory (ROM) containing the operating system and built-in applications and

4) built-in flash memory. See also non-volatile memory.

MMC

Short for "Multi-Media Card". Similar in form factor to an SD card. The difference between an SD card and an MMC card is speed, durability, write-protection, copyright protection, and size.

Modem

Short for "modulator-demodulator". A modem is a device or program that enables a computer to transmit data over, for example, telephone or cable lines. Computer information is stored digitally, whereas information transmitted over telephone lines is transmitted in the form of analog waves. A modem converts between these two forms. There is one standard interface for connecting external modems to computers called RS-232. While the modem interfaces are standardized, a number of different protocols for formatting data to be transmitted over telephone lines exist.

NFC Short for "Near Field Communication". NFC is a wireless connectivity technology that enables short-range communication between electronic devices. If two devices are held close together (for example, a mobile phone and a personal digital assistant), NFC interfaces establish a peer-to-peer protocol, and information such as phone book details can be passed freely between them. NFC devices can be linked to contactless smart cards, and can operate like a contactless smart card, even when powered down. This means that a mobile phone can operate like a transportation card, and enable fare payment and access to the subway.

NFC is an open platform technology standardized in ECMA (European Computer Manufacturers Association) 340 as well as ETSI (European Telecommunications Standards Institute) TS 102 190 V1.1.1 and ISO/IEC 18092. These standards specify the modulation schemes, coding, transfer speeds, and frame format of the RF interface of NFC devices, as well as initialisation schemes and conditions required for data collision-control during initialisation – for both passive and active modes.

OSI Short for "Open System Interconnection". The OSI model defines a networking framework for implementing protocols in seven layers.

PC Short for "Personal Computer". A PC is a single-user computer based on a microprocessor. In addition to the microprocessor, a personal computer has a keyboard for entering data, a monitor for displaying information, and a storage device for saving data.

PCMCIA

Short for "Personal Computer Memory Card International Association". The PCMCIA is an international trade association and standards body cognisant of several device standards including PC Cards, Miniature Card, and others. PCMCIA is also used to describe PC Cards themselves, often referred to as PCMCIA Cards.

PDA

Short for "personal digital assistant". A PDA is a handheld device that combines computing, telephone/fax, Internet and networking features. A typical PDA can function as a cellular phone, fax sender, Web browser and personal organizer. Unlike portable computers, most PDAs began as pen-based, using a stylus rather than a keyboard for input. This means that they also incorporated handwriting recognition features. Some PDAs can also react to voice input by using voice recognition technologies. PDAs of today are available in either a stylus or keyboard version.

protocol

An agreed-upon format for transmitting data between two devices. The protocol determines the following:

- the type of error checking to be used
- data compression method, if any
- how the sending device will indicate that it has finished sending a message
- how the receiving device will indicate that it has received a message

RJ-45

Short for "Registered Jack-45". RJ-45 is an eight-wire connector used commonly to connect computers onto a local-area networks (LAN), especially Ethernets. RJ-45 connectors look similar to the ubiquitous RJ-11 connectors used for connecting telephone equipment, but they are somewhat wider.

RFID

Short for "Radio Frequency Identification". An RFID device interacts, typically at a limited distance, with a "reader", and may be either "passive" (powered by the reader) or "active" (having its own power source, such as a battery).

SD

Short for "Secure Digital". SD is a technology standard for providing portable devices with non-volatile memory/storage and peripheral I/O expansion capability. On some devices this standard is implemented in the form of SD memory expansion cards, used to store digital information like applications, databases, photos, text, audio, video or MP3 music files, and an SD/SDIO expansion slot. The SD standard makes it possible to transfer information between devices that support SD expansion cards (e.g. transfer photos between a digital camera and a PDA by exchanging the SD expansion card), assuming both devices support the file format used for the transferred information (e.g. JPEG image file).

SDIO

Short for "Secure Digital Input/Output". SDIO is a part of the SD memory specification. It enables I/O (input/output) expansion for add-ons such as serial, modem, camera or GPS (global positioning system) cards. Whereas SD is only used for storage expansion cards, an SDIO capable expansion slot can also support SD expansion cards, while an SD-capable slot may not support an SDIO expansion card.

SIM

Short for "Secure Identity Module" or "Subscriber Identification/Identity Module". A SIM card inscribed with a customer's information and designed to be inserted into any mobile telephone. Usually SIM card phones work by GSM technology. The SIM card contains a user's GSM mobile account information. SIM cards are portable between GSM devices— the user's mobile subscriber information moves to whatever device houses the SIM.

SAM

Short for "Secure Application Module". A SAM a hardware module within a transaction device (e.g. smart card terminal) that controls all security related transaction and communication between the device and the web, PC, etc. The SAM can only be accessed by the scheme operator, it is usually tamper proof for everybody else software Computer instructions or data. Anything that can be stored electronically is software. Software is typically stored in binary form (ones and zeros, represented by two distinctive states) on a storage medium, such as a floppy disc, hard drive, memory device, or the like, all of which may generally and broadly be referred to as "hardware". The apparatus or system or device which responds to software instructions or manipulates software data may generally and broadly be referred to as a "computer". Software is sometimes abbreviated as "S/W". Software is often divided into the following two categories:

- systems software : Includes the operating system and all the utilities that enable the computer to function.
- applications software : Includes programs that do real work for users. For example, word processors, spreadsheets, and database management systems fall under the category of applications software.

software The non-hardware part of a computer, handheld (e.g., PDA) or smartphone ("smart" cellular telephone) consisting of instructions used to operate these devices. Includes applications that are added to, or included on, the device, as well as the operating system built into a device.

SSL Short for "Secure Sockets Layer". SSL is a secure tunnel that is created automatically when a user connects to a page that requires secure data transmission. (i.e., any page whose URL begins with https://)

TCP/IP Short for "Transmission Control Protocol/Internet Protocol". TCP/IP has become the basic protocol that defines how information is exchange over the Internet. IP software sets the rules for data transfer over a network, while TCP software ensures the safe and reliable transfer of data. The abbreviation TCP/IP is commonly used to represent the whole suite of internetworking software.

TDMA Short for "Time Division Multiple Access", a technology for delivering digital wireless service using time-division multiplexing (TDM). TDMA works by dividing a radio frequency into time slots and then allocating slots to multiple calls. In this way, a single frequency can support multiple, simultaneous data channels. TDMA is used by the GSM digital cellular system.

tamper-resistant area An area, within a memory device which is hardware protected against tampering. A pure software approach to tamper with the tamper-resistant area will not work.

UDP Short for "User Datagram Protocol". UDP is a minimal message-oriented transport layer protocol.

URL Short for "Uniform Resource Locator". Web pages use links to connect users to other content that may or may not be located on the same server as the page from which it links. The address used to identify the location of this content is called a URL.

USB Short for "Universal Serial Bus". USB is a serial bus standard (standardized communications protocol) that enables data exchange between electronic devices. USB supports data transfer rates of up to 12 Mbps (megabits per second). A single USB port can be used to connect up to 127 peripheral devices, such as mice, modems, and keyboards. USB also supports plug-and-play installation and "hot plugging". USB is expected to completely replace serial and parallel ports. Hi-Speed USB (USB 2.0) similar to FireWire technology, supports data rates up to 480 Mbps.

- A USB flash memory drive is a portable storage device, which functions like a hard drive or a removable drive when inserted into the USB port of a PC.

Primarily used to store, backup, download and transfer data from one computer to another. These USB key chain memory devices have replaced floppy disk drives in the market.

- A USB Token is a portable, hand-held key fob that is the size of a standard car key. It is embedded with a computer microchip that can store, access and process data. USB tokens have an operating system, temporary memory and non-volatile, "updateable" file/object storage memory, affording capabilities greater than those of traditional smart cards. They can generate secret cryptographic keys (Public & Private Key Infrastructure) and store private data (digital certificates, digital signatures, biometric identifiers, passwords, system settings etc).

UWB UWB is short for "Ultra Wide Band". UWB is a wireless communications technology that transmits data in short pulses which are spread out over a wide swath of spectrum. Because the technology does not use a single frequency, UWB enjoys several potential advantages over single-frequency transmissions. For one, it can transmit data in large bursts because data is moving on several channels at once. Another advantage is that it can share frequencies that is used by other applications because it transmits only for extremely short periods, which do not last long enough to cause interference with other signals.

VPN Short for "Virtual Private Network". A VPN provides a way to remotely and securely access a corporate network via the Internet. VPN is an Internet-based system for information communication and enterprise interaction. A VPN uses the Internet for network connections between people and information sites. However, it includes stringent security mechanisms so that sending private and confidential information is as secure as in a traditional closed system. A network which has the appearance and functionality of a dedicated line, but which is really like a private network within a public one, because it is still controlled by the telephone company, and its backbone trunks are used by all customers.

Wi-Fi Short for "Wireless Fidelity". Wireless technology, also known as 802.11b, that enables you to access the Internet, to send and receive email, and browse the Web anywhere within range of a Wi-Fi access point, or HotSpot.

wireless Technology that allows a user to communicate and/or connect to the Internet or mobile phone networks without physical wires. Wi-Fi, Bluetooth®, CDMA and GSM are all examples of wireless technology.

WLAN Short for "wireless local-area network". Also referred to as LAWN. A WLAN is a type of local-area network that uses high-frequency radio waves rather than wires for communication between nodes (e.g., between PCs).

BRIEF DESCRIPTION (SUMMARY) OF THE INVENTION

The invention is generally a compact personal token apparatus which can be plugged into a personal computer and interfaced with the virtual world of the Internet. The apparatus (or, as will be evident, a portion of a modular apparatus) can then be removed from the personal computer and used to conduct real world transactions. The compact personal token apparatus is suitably in the general form of a fob, resembling a USB memory fob.

The compact personal token apparatus comprises a wireless interface.

With regard to a personal token apparatus being something "which can be plugged into a personal computer", it is clearly within the scope of this invention, and based on the teachings set forth herein one of ordinary skill in the art would recognize that:

- the "token apparatus" can take on a form other than that of resembling a USB memory fob, as long as it is minimally capable of storing software (data and/or instructions); and
- the "personal computer" can be any apparatus which is capable of interacting with the token apparatus (or the like), so long as the apparatus is a device capable of interacting with the software contained in the token apparatus (or the like).

In light of these considerations, and other comparisons (an exemplary "other comparison" would be the well-accepted definition of "software" set forth hereinabove which defines "software" as the non-hardware part of a computer, handheld or smartphone ...) set forth in this document, the preceding paragraph (i.e., " The invention is generally ... comprises a wireless interface.") can reasonably and justifiably be read and interpreted as follows:

The invention is generally a compact personal token apparatus which can be by means of standard-compliant interfaces (described hereinbelow) connected to a personal computer and/or other internet capable devices such as; cell phones, personal digital assistants (PDA), digital media players, digital cameras etc. and interfaced with the virtual world of the Internet. The apparatus (or, as will be evident, a portion of a modular apparatus) can then be removed from the personal computer and used to conduct real world transactions. The compact personal token apparatus is suitably in the general form of a fob, resembling a USB memory fob. In some implementations it will take the general form factor required of the standard compliant interface such as SD and Mini SD cards, Multi Media Cards (MMC), PCMCIA Cards, etc. The compact personal token apparatus generally comprises a wireless interface.

According to a feature of the invention, the compact personal token apparatus (or equivalent) may remain in the apparatus capable of interacting with the personal token (e.g., cell phone, PDA), when the personal token device communicates contactlessly (e.g., wirelessly) in the real world. It does not necessarily have to be removed from the host device.

According to the invention, a compact personal token apparatus comprises a connection module; a translation module; a processor module; and an input/output module. The connection module is for interfacing the personal token apparatus with a an Internet-capable appliance; and the interface is selected from the group consisting of USB, FireWire, IR, Bluetooth, standard serial port, WLAN. The Internet-capable appliance may comprise a device selected from the group consisting of personal computer (PC), laptop, PDA, MP3 player and cellphone. The translation module moves signals between a USB interface and a smart card interface. The smart card interface may be selected from the group consisting of ISO 7816, ISO 14443 and ISO 15693.

The processor module may comprise a dual interface (DI) chip. The processor module may incorporate the translation module. The output module comprises an RF antenna and a modulator. The apparatus may further comprise flash memory. The translation module may move signals between a USB interface and a wireless interface. The translation module may be incorporated in the processor module to that the device can go directly from USB to wireless without being limited by smart card software architecture limitations. The apparatus may have the general physical configuration of a conventional USB memory fob. The apparatus may be modular, having a first physical module containing the input module and the translation module; and a second physical module containing the processor module and the output module. The output module may comprise contacts for interfacing with a smart card. The fob is capable of interfacing with the Internet and emulating a smart card. The apparatus may incorporate firewall functionality to protect the Internet-capable applicance. The apparatus may comprise interfaces for ISO contact, contactless, USB and DSL. The apparatus may comprise an LCD screen. The apparatus may comprise at least one switch. The apparatus may comprise at least one LED.

According to the invention, a compact personal token apparatus comprises a standard–compliant contact based interface, the contact based interface complying to at least one standard interface selected from the group consisting of USB, IEEE 1394, PCMCIA, Compact Flash, Multi Media, Memory Stick, Smart Media, Secure Digital, mini SD, IBM Micro Drive, and any similar standard interface.

The apparatus may further comprise a standard–compliant contactless/wireless interface; the contactless/wireless interface complying to one or more of the following standard interfaces: RFID-contactless interface according to ISO 14443 and ISO 15693 as well as similar interfaces, Bluetooth compatible interface, WLAN 812.11, UWB, and any similar interface.

The apparatus may further comprise a standard-compliant interface releaseably coupleable to a host processing device, this being under the command of an operating system; an interface module providing translation of standard-compliant contact based interface messages to ISO 7816 compliant messages and providing the translation of ISO 7816 compliant messages to standard-compliant contact based interface messages; a dual interface processor having an ISO7816 compliant interface communicating through the interface module with the host processing device, the dual interface processor communicating through an RFID-contactless interface and connected to an inductive antenna.

The apparatus may further comprise a standard-compliant interface releaseably coupleable to a host processing device, this being under the command of an operating system; an interface module providing translation of standard-compliant contact based interface messages via a memory chip to Bluetooth /WLAN 812.11 device compatible compliant messages, and providing the translation of Bluetooth /WLAN 812.11 device compliant messages via a memory chip to standard-compliant contact based interface messages; a Bluetooth /WLAN 812.11 device having a Bluetooth/WLAN 812.11 compliant interface communicating through the interface module with the host processing device via a memory chip; the same Bluetooth /WLAN 812.11 device communicating through its Bluetooth /WLAN 812.11 compatible interface.

The apparatus may further comprise a dual interface chip (processor) inside the personal token which can be directly programmed by a software running on the host system using the interface processor without the need for an external contact based dual interface read/write device. The software may be web based, allowing for downloading information from the web directly into the dual interface processor memory (for example, event tickets) thus linking the virtual world to the real world. The downloaded information may be used in the real world by using the contactless RFID interface.

The information stored in the personal token via the standard contact based interface may be used for personal identification, secure network logon, access control, e-ticketing, e-payment and similar applications using either the standard compliant interface or the RFID-compliant interface. Information received through the RFID- interface can be stored in the memory of the personal token and can then be provided to the host processing device via the standard interface, thus allowing a complete information exchange between the virtual world and the real world.

The contactless / wireless module may be releaseably coupleable from the interface module.

The dual interface processor may be mounted in a dual interface card complying to ISO 7810 or a 7816 compliant SIM module and connected norms; the compact personal token apparatus provides physical contacts for the dual interface card, or a 7816 compliant form factor; and when connected, the dual interface or SIM card can communicate with the host processing device through the interface module inside the personal token and, once the communication is done, the card can be released from the personal token and can be used then in the real world.

The apparatus may further comprise a processor module; and additional memory selected from the group consisting of flash memory and EEPROM device powered and addressed by the processor module; wherein the additional memory can be used for user authentication and to run applications.

The apparatus may further comprise a standard–compliant smart card contact interface complying to ISO 7816, or any similar interface.

The apparatus may further comprise a connection module, connecting the personal token apparatus to a host device such as PC, PDA, smart cellular phone or similar device, either directly or with the help of a standard reader device such as a memory card reader.

The apparatus may further comprise a standard-compliant interface releaseably coupleable to a host processing device, this being under the command of an operating system; and a translation module, translating messages incoming from the contact based interface, and translating messages to the host device from the personal token apparatus.

The apparatus may further comprise a processor module, preparing messages to be sent by the contactless/wireless interface of and interpreting messages received via the interface.

The apparatus may further comprise a triple interface (e.g., contact, contactless, USB) processor.

The apparatus may further comprise a quadruple interface (e.g., contact, contactless, USB, DSL) processor.

According to the invention, a method of interacting wirelessly comprises: providing a device; interfacing the device with a an Internet-capable appliance; and providing a smart card interface in the device.

The "compact personal token apparatus" may be referred to herein as "smart fob" (without prejudice to any trademark rights which may be claimed). Often it is simply referred to as the "apparatus" (no trademark rights implied). Various embodiments and methods of use are disclosed.

It will be appreciated that the "smart fob" of the present invention is not only capable of functioning like a smart card, but is also capable of much more.

The "smart fob" is capable of loading and storing information from the Internet, via a PC or other Internet capable device to its memory and then using the stored information via its wireless interface in the real world. The "smart fob" is also capable of exchanging information with a conventional smart card.

Based on the teachings set forth herein, it would readily be understood by one of ordinary skill in the art that the functionality of the present invention, in its various embodiments, could be realized in a different format than a fob and in a different manner than by plugging the fob into the USB port of a personal computer (PC). For example, the apparatus of the present invention can be embodied in a format (form factor) such as that of an SD (secure digital) card which can be plugged into any device having an appropriate interface for inserting an SD card, such as a laptop, palmtop, cell phone, digital camera, personal digital assistant (PDA), MP3 player, or the like.

In any of the embodiments discussed herein (particularly those using a PC), a memory card reader may be attached to the PC. (PCs in Europe commonly come with memory card readers for several different memory card formats including, but not limited to, Secure Digital (SD) card format

Many exemplary features and embodiments of, as well as applications for the smart fob (or comparable) of the present invention are described hereinbelow.

Other objects, features and advantages of the invention will become apparent in light of the following description thereof.

BRIEF DESCRIPTION OF THE DRAWINGS

The structure, operation, and advantages of the present preferred embodiment of the invention will become further apparent upon consideration of the descriptions set forth herein, taken in conjunction with the accompanying figures (FIGs). The figures (FIGs) are intended to be illustrative, not limiting. Although the invention is generally described in the context of these preferred embodiments, it should be understood that it is not intended to limit the spirit and scope of the invention to these particular embodiments.

FIG. 1A is a schematic block diagram of an embodiment of the invention.

FIG. 1B is a schematic block diagram of an embodiment of the invention.

FIG. 1C is a schematic block diagram of an embodiment of the invention.

FIG. 2A is a perspective view of an embodiment of the invention.

FIG. 2B is a perspective view of an embodiment of the invention.

FIG. 3A is a perspective view of an embodiment of the invention.

FIG. 3B is a perspective view of an embodiment of the invention.

FIG. 4 is a schematic block diagram of an embodiment of the invention.

FIG. 5 is a schematic block diagram of an embodiment of the invention.

DETAILED DESCRIPTION OF THE INVENTION

This invention relates generally to devices, technology and applications for downloading and interacting with data and value from one "world" such as the virtual world of the Internet and, with the device, interacting, typically wirelessly, with another "world" such as the physical world of banking, stores (point of sale), physical access control, and the like.

Generally, this is done using a device running software and interacting with an Internet capable apparatus such as a personal computer (PC), a personal digital assistant (PDA) or a handset (Internet capable cell phone). In many embodiments, the device interacts with the physical world using a standard wireless smart card interface, such as ISO 14443 or 15693. In some embodiments, the device plugs into a PC using a standard contact interface, such as USB. Several embodiments and several applications applicable to various ones of the embodiments are discussed.

In an embodiment, the device is embodied in the form of a compact personal token apparatus, resembling a conventional USB memory fob (size, shape, form) which can be plugged into an apparatus such as a personal computer (PC) and interfaced with the virtual world of the Internet. The device is capable of loading and storing information from the Internet, via the PC to its flash memory (memory that can be erased and reprogrammed in blocks) or EEPROM and then using the stored information or value via its wireless interface in the real world. Similarly, the device is capable of implementing an auto-run application, when inserted into a personal computer (PC) connected to the Internet, and information exchanged and stored can be accessed in the real world application via its wireless interface. The memory space required for the auto-run application can reside completely in the device or only partially in the device. Additional memory space to complete the application can be located on the server of the ISP, trusted third party or host server. The apparatus is also capable of exchanging information with other devices having compatible interfaces.

The personal token apparatus will typically be referred to as a "device" to distinguish it from the "apparatus" that it plugs into. However it may occasionally still be referred to as "apparatus". Also the apparatus that the device plugs into to interact with the virtual world may also sometimes be referred to as "device", and may also be referred to as "appliance". Generally, the context will clarify the definition.

FIG. 1A is a schematic block diagram of an exemplary embodiment 100 of the invention employing a dual interface (DI) chip and having four modules, all interconnected as shown to provide the contemplated functionality of the present invention. The major components, mounted on a circuit board (PCB, not shown) and within a housing (not shown) are (from left-to-right):

- a connection module 102;
- a translation module 104;
- a processor module 106; and
- an input/output (I/O) module 108.

The connection module 102 is for interfacing the device with a personal computer (not shown) apparatus, or other appliance capable of communicating and interacting with remote servers and networks. In the example of the compact personal token apparatus of the present invention, the connection module can be a USB plug, for plugging directly into a personal computer (PC). Other possibilities for connecting (communicating) with the personal computer are FireWire, IR, Bluetooth, standard serial port, WLAN, etc., basically any suitable interface between an external memory/processing apparatus and a personal computer.

The connection module 102 is typically for inputting data to the device from the virtual world of the Internet, via the PC or other Internet capable appliance, and in some cases the device can or needs to also output data to the PC and/or to another entity via the Internet. The particular plug or connection interface which is used is whatever is available, either now or in the future. And the device is not limited to communicating with other entities via the "Internet", but can communicate via other networks or internets. These comments apply to other embodiments described herein.

The invention should not limited to a particular form of interface/communication protocol. The point is that the device can interact with the virtual world via an Internet-capable appliance. One of ordinary skill in the art to which the invention most nearly pertains will recognize, and it is within the scope of the invention that other possibilities for what has been described as "devices capable of communicating and interacting with remote servers and networks" are PDAs, cell phones, etc., not only personal computers - basically, any (what is referred to elsewhere as) "host device" or "host processing device".

The translation module 104 is for going (moving signals) from USB (the exemplary interface with the computer) to a smart card interface format, such as ISO 7816, and vice-versa. The translation module may comprise a Philips TDA8030 USB/7816. (ISO 7816 is a smart card contact interface.)

A micro-controller such as an 8 bit micro-controller (ST7 FSCR1E4M1) can be used as an interface translator chip (104) between the USB connection 102 and the processor module 106. (The processor could be mounted in a SIM module.)

Alternatively, the translation module can go from USB to ISO 14443 or 15693 (wireless interfaces). The latter is shown in **FIG. 1B**, and is described hereinbelow. In going directly from USB to wireless, the device is not limited by the smart card software architecture (ISO

7816) limitations. The translation module in this case is a processor device, that will handle the data processing from USB to wireless.

The processor module 106 is for controlling operation of the compact personal token apparatus ("device") of the present invention and is preferably capable of operating as a dual-interface (DI) chip. For example, Mifare ProX, Infineon 66 series, etc. The dual interface chip is available from various vendors (e.g., Philips, Infineon, ST Microelectronic), and is capable of interfacing from ISO 7816 (contact interface) to either or both of ISO 14443 and 15693 (wireless interfaces).

The output module 108 comprises an RF antenna and a modulator, etc. Alternatively, the output module comprises a set of contacts for contacting the pads on a smart card (see **Figures 3A** and **3B** below).

It should clearly be understood that, in this as well as in other embodiments described herein, that the module 108 is more than an "output" module sending data in only one direction, that rather it is a transceiver module adapted to transmit as well as receive data. The same can be said of the input module (e.g., 102 in that it facilitates two-way communication. It is only as a prosaic convenience that the modules 102 (e.g.) and 108 (e.g.) are labeled "input" and "output" respectively.

As mentioned above, alternatively, the translation module can go from USB to ISO 14443 or 15693. In other words, directly from USB to wireless.

FIG. 1B is a schematic block diagram of another exemplary embodiment 120 of the invention, also having four modules, all interconnected as shown to provide the contemplated functionality of the present invention. The major components, mounted on a circuit board (PCB, not shown) and within a housing (not shown) are (from left-to-right):

- a connection module 122;
- a translation module 124;
- a processor module 126; and

- an input/output (I/O) module 128.

As in the previous embodiment, the connection module 122 can comprise a USB plug or any suitable interface to a personal computer or other device (apparatus, appliance) capable of communicating and interacting with remote servers and networks.

As in the previous embodiment, the output module 128 can comprise an RF antenna and modulator, or alternatively a set of contacts for contacting the pads on a smart card.

Unlike the previous embodiment, in this embodiment the translation module 124 goes from USB to a wireless interface. Therefore, the processor module 126 does not need to be a dual interface (DI) chip. Rather, the processor module 126 could simply comprise a USB interface on one side and a wireless interface on the other. The memory of the processor could be used as temporary storage and the processor could handle the data encoding as well.

It is also within the scope of the invention that the processor module (e.g., 106 or 126) could include (incorporate) the translation module (e.g., 104 or 124) within the processor module itself, thus enabling an even more cost effective solution, enabling using a single chip approach for some, or even all of the embodiments discussed herein. (This is not explicitly shown, but one could envision, for example, simply merging the blocks 124 and 126 together, as indicated by the dashed line.)

FIG. 1C is a schematic block diagram of another exemplary embodiment 140 of the invention, based on the embodiment 100 of **FIG. 1A**. The major components are:

- a connection module 142;
- a translation module 144;
- a processor module 146; and
- an input/output (I/O) module 148.

In this embodiment 140, a flash memory device 150 can be included, with a storage capacity of 1 to 4 megabytes (or more) for the purpose of running applications. The memory management for the device may be handled by a crypto controller operating system with an 8 bit address bus in the dual interface (DI) chip. The flash memory device may be any suitable device including, but not limited to, Secure Digital (SD) card format, and including SIM card. (A crypto controller is a processor chip capable of encrypting and decrypting data to be stored in internal or external memory.)

The functionality of the invention has been described hereinabove. Various applications for the invention will be described hereinbelow. Meanwhile, exemplary physical forms of the invention will be described.

The invention may be embodied in the form of a "smart fob" apparatus, having the general physical configuration (size, shape, form) of a conventional USB memory fob. Refer to **FIG. 2A**. This is basically a device 200 having the elongate size and general shape of your finger, comprising a main body portion 210 housing the electronics (cf. 104,106,108) and a USB plug 212 (cf. 102) extending from an end of the body portion 210. A hole 214 may be provided for suspending the device 200 from a keychain (not shown).

As mentioned above, the "compact personal token apparatus" may be referred to herein as "smart fob" (without prejudice to any trademark rights which may be claimed). Now that its functionality has been described ("smart") and an exemplary physical form ("fob") has been described, the device will typically be referred to simply as the smart fob (without quotation marks).

Figure 2B illustrates another exemplary embodiment 220 of the smart fob, again in the general form of a USB memory fob. But in this case, the smart fob has a first physical module 222 (left, as viewed) which contains the input module (e.g., 102, USB plug, cf. 212) and translation module (e.g., 104), and a second physical module 224 (right, as viewed) which contains the processor module (e.g., 106, dual-interface chip) and output module (e.g., 108, RF antenna and modulator). The two modules 222 and 224 can plug together and be taken apart from one another. In this manner, after interacting with the "virtual world" on his computer, the user can separate the two modules 222 and 224 and carry just the second module, for conducting "real world" transactions. The second module 224, comprising processor and output module, is sufficient for conducting real world, wireless transactions, in the manner of a smart card. In other words, the smart fob can emulate a smart card.

Figure 3A illustrates another exemplary embodiment of the invention wherein, rather than being intended to function as (emulate) a smart card, the output module (e.g., 108) of the compact personal token apparatus 300 is adapted to receive and communicate with a standard (including dual interface) ISO 7810 (7816) smart card 310. Instead of an RF antenna (and modulator), the fob 300 would have contacts for interfacing with the contact pads of the smart card 310.

The fob of this embodiment could be modularized, as shown in **Figure 3B**, having a first physical module 322 comprising the input module (e.g., 102) and translation module (e.g., 104) and a second physical module 324 comprising the processor module (e.g., 106) and the output module (having contacts rather than antenna/modulator), although the purpose of modularization in this case would not be for carrying around, but rather for changing/updating components. Or, the **Figure 2A** or **2B** embodiments could be modified by just adding a contact reader slot for a smart card. In this case, the compact personal token apparatus functions as more than a reader, it is a transaction device.

Normally, the **Figure 3A/3B** product would not require the DI chip (e.g., 106) and the RF interface (e.g., 108). However, if it does, when connected to a PC it could be used to load value stored on a smart card onto the smart fob, and then use that value in the real world. Now you have the ability to add value and information or exchange value and information between the fob and a conventional contact smart card.

Also if the **Figure 3A/3B** product would contain the chip and the RF interface you could use it – when connected to a PC - to load value stored on a smart card and then use that value in the real world. This provides the ability to add value and information to the smart fob from smart cards as well as from the Internet. An example would be a cash transaction between two people – a person with a smart card could transfer the purchase amount of an item to the smart fob via the 7816 interface and the owner of the smart fob could take the smart fob to a fast food restaurant and use the stored value to buy lunch. In these cases, the **Figure 3A/3B** embodiment is not simply a smart card reader.

In a variation on the above, combining (so to speak) **FIGs. 2B** and **3B**, a modular smart fob could be sold having the left hand portion 222 (or 322) of the two devices 220, 320, plus the right hand portion 224, plus the right hand portion 324 so that the device could function both as a smart card (with RF interface) and as a smart card reader (with contacts for reading/writing smart cards), in addition to its functionality derived from plugging into a PC and interacting with the virtual world via the Internet.

FIG. 4 is a schematic block diagram of an exemplary embodiment 400 of the invention wherein the device can be used as a firewall to protect, for example, a PC. The functionality is described elsewhere in greater detail. The principal components of the device 400 are:

- a connection module 402 for plugging into the USB (or, network, LAN/Ethernet, or Fast Ethernet 10/100 MBit) port of a PC;
- a processor module 406; and
- an input module 408 which, unlike other embodiments, need not perform wireless functions, but rather is socket (or plug), such as RJ-45, for connecting to a telephone line (or the like) supporting a DSL (or the like) connection to the Internet.
- The device 400 may also incorporate flash memory 510 (compare 150).

FIG. 5 is a schematic block diagram of an exemplary embodiment 500 of the invention, based on the embodiment 100 of **FIG. 1**. The major components are:

- a connection module 502;
- a translation module 504;
- a processor module 506;

- an input/output (I/O) module 508; and

- an LCD display 510 for displaying messages regarding status or other relevant information to the user. It will be understood that a device having an LCD display should be "active", having its own battery (not shown).

Other input and output devices, such as switches 512 and LEDs (light-emitting diodes) 514, could readily be added to the device.

The smart fob of the present invention can be implemented in forms other than that of resembling a conventional USB key fob, including single chip solutions, multichip modules, a form resembling that of a flash memory device such as an SD card, and the like. The form that the invention takes is largely dictated by the apparatus with which it is intended to interface. For a PC, a USB fob is ideal. For an Internet capable mobile phone, a SIM card or SD card format may be preferable.

Applications/Use

In use, for example, the user plugs the smart fob into his PC, or other Internet capable device (appliance), connects to the Internet, and interacts with a service or content provider to upload and/or download information. For example, downloading a ticket. Then, the user takes the smart fob to the event where it connects wirelessly with a reader at the venue to allow entrance and stamp the ticket (e.g., set a flag indicating that the ticket was used).

In another example, a consumer can use the smart fob to store "e-coupons" on the smart fob – loaded via the Internet. Then taking the smart fob to a participating merchant, use the coupons to receive a savings or price reduction on the product.

In another example, a consumer could load cash value to the smart fob via the Internet and use the cash in the real world – at participating merchants – to buy a meal, newspaper, etc.

In another example, which can be called "kids fob" (also, without prejudice to potential trademark rights) – parents can provide their young children with a smart fob loaded with a preset amount of cash and send them off to the mall or participating theatre and know that the money will be used as intended.

In another example, a consumer could use the smart fob to load cash via the internet – and while still connected to the PC use the stored value to pay cash for products or services on the internet. This addresses the concern that consumers still have some reservations about giving out their credit card information over the Internet.

In another example, a consumer could load award certificates onto the smart fob earned from a merchant loyalty program and then take the smart fob to a retail store to redeem for merchandise - no more waiting for mailed certificates.

In another example, the smart fob could store a biometric - such as fingerprint, iris scan etc., in a memory cell that is locked and when using the smart fob to gain access to a controlled area, the user touches his finger to a reader, waves the smart fob in front of a reader, the finger print is compared to the stored info, the user's identity is verified, and he is granted access.

Another exemplary application for the smart fob would be Electronic Learning. Typically, a student has to download a lot of information from the University in the course of any course of study, needs passwords to enter external databases, and needs a swipe card to use a photocopier or even pay at the school cafeteria. Also, access to the library is restrictive. In short, the smart fob of the present invention could be used to store files, access networks, download secure sealed PDF files, access buildings and make payment for services. Upon admission, all of the information could be ported to the student's smart fob.

In general, applications for the smart fob comprise substituting smart cards with the smart fob in a multiple of applications such as automatic fare collection in mass transit, paperless event & travel ticketing, loyalty programs, coupon redemption, cashless payment and online services.

The smart fob can operate as a security device. For example, the smart fob starts an auto-run application, after insertion in an Internet-connected PC. In simple terms, the PC user is automatically connected to a participating merchant's website and can conduct a business transaction in a secure fashion, without the fear of anyone spying or manipulating the data. This requires the the creation of a virtual private network (VPN) tunnel from the user's PC over the public infrastructure to the ISP (Internet Service Provider) or Trusted Secure server via a firewall, and after user authentication, providing the direct link to the host server. The VPN software is embedded into the smart fob and loaded onto the firewall appliance to create the gateway and to protect the ISP or Trusted Secure server. In essence, the smart fob provides the firewall protection for the home PC user, whereby the screening software resides in the firewall appliance. The embedded software in the device is field upgradeable, meaning that the cryptographic and application software can be updated online anytime.

Multi-applications are feasible with a single smart fob device, but it also envisaged that a PC user could have a specific "smart fobs" from each of his or her preferred travel agent, airline, hotel chain, car rental, financial institute, media concern, book & music store, entertainment provider, retailer, lottery operator, etc.

The smart fob device provides convenience, flexibility and enhanced transaction speed. It performs all of the same functions as a traditional smart card, but it is a "readerless" solution in the home environment (eliminating the primary barrier to smart card adoption by consumers). Simple and effective – all the user needs to do is plug the device into the USB port in the home PC and download eCash, tickets or coupons.

In use, for example, the user plugs the smart fob device into a PC, connects to the Internet, and interacts with a service or content provider to upload and/or download information. For example, the user can download an event ticket, take the device to the venue, just wave the device in close proximity to a turnstile equipped with a wireless reader at the entrance, and access is granted without having to stand in line.

In another example, a consumer can load cash to the electronic purse of the smart fob device via Internet banking, and while still connected to the PC use the stored value to pay for online products or services.

Equally, a consumer can load electronic cash to the smart fob device and use the e-cash at participating merchants to pay for food and beverages. No hassle with cash, tickets or queues!

In another example, a consumer can visit a participating merchant's website and download "e-coupons" to the smart fob device. At the retail (e.g., grocery) store, the consumer can redeem the coupons for savings on their purchases. At the checkout the consumer purchases are scanned and checked against the database of stored e-coupons in the smart fob device. The value of the coupons is decremented off the device and the savings amount is passed to the cash register to deduct from the total bill.

In another example, a consumer can load award certificates onto the device earned from a merchant loyalty program and then redeem them for merchandise at the store.

As mentioned above, the smart fob (device) is capable of implementing an auto-run application, when inserted into a personal computer (PC) connected to the Internet, and information exchanged and stored can be accessed in the real world application via its wireless interface.

In the auto-run application, the smart fob can function as a portable client user that can be inserted into any Internet connected PC having Windows 2000, Windows XP or Linux operating system with activated firewall. Information is exchanged over the Internet via the TCP/IP (Transmission Control Protocol/Internet Protocol) protocol and protected, for example by SSH (Secure Shell) encryption for remote login. A VPN (Virtual Private Network) cryptographic tunnel for secure information communication over the public infrastructure to the ISP (Internet Service Provider), the Trusted Secure server or directly to the Host server is initiated when the smart fob is inserted into the PC. The process "point-to-point tunnelling" means that packets of data are encrypted and wrapped inside IP (Internet Protocol) packets so that non-IP data can travel through the Internet. The Secure Shell solves the security problem of hackers stealing passwords and attacks such as IP spoofing, IP source routing and DNS spoofing.

The VPN software is loaded onto the smart fob and onto the firewall appliance to create the gateway and to protect the ISP or Trusted Secure server.

The secure tunnel for secure information communication over the public Internet to the ISP (Internet Service Provider) is initiated when the smart fob is inserted into the PC, a feature provided by the auto-run functionality. The embedded static IP address locates the ISP or Trusted Secure server.

The selection of IPsec (short for IP Security), which operates at layer 3 of the OSI model, makes it suitable for protecting non-IP packets, for example UDP traffic as compared with transport-layer protocols such as SSL, which cannot protect UDP level traffic.

The client user can be authenticated by the ISP or by a trusted third party through a digital signature or a unique MAC (Media Access Control) address, or through the implementation of public key infrastructure in order to validate the client's identity.

By passing through an ISP or in-house secure server with virus scan and filter, Spam, Trojan Horses, Worms or Pop-Up Windows can be blocked. After authentication is successfully verified, a direct link with the host server is established.

Therefore, the smart fob can be viewed as a marketing platform that encapsulates auto-run application software for a specific application, a USB apparatus for memory management and radio frequency identification, mass storage capability, a secure server for authentication and filtering as well as a wireless interface, to provide a myriad of solutions addressing marketing, e-commerce, business productivity, IT (information technology), consumer, communication, content, security and mobility issues.

The smart fob can be used as a payment device for retail purchase & loyalty with the Internet feature allowing users to download value, coupons, tickets, entertainment content, etc. The smart fob can be personalised like a conventional credit/debit card for electronic payment and the wireless interface feature can be used for photo identification, to download transit & event tickets, to receive complimentary coupons, loyalty points, gift certificates and messages, for vending and to redeem coupons. In addition the smart fob eliminates the need to tender with cash.

For example, by simply inserting the smart fob into the USB port of a telephone linked PC, an automatic Internet connection to the website of the user's favourite airline is established, via a secure server to authenticate the user and block spam, viruses, and SMTP (simple mail transfer protocol) based attacks. Personal data, frequent flyer miles as well as credit card details can be encrypted and stored in the smart fob. Tickets can also be downloaded onto the smart fob and used in contactless mode at the airline check-in desk. This "client user to secure server to host server" concept blocks pop-up windows, viruses, worms, spam and Internet "phishing" fraud. The airline can use the platform to attract other merchants that compliment the airline's product portfolio.

For a smart fob with on-board battery power and a display (e.g., a small one or two line LCD display panel), the seat reservation number can be stored on the display.

A consumer can load funds from their bank account via the Internet to the ISP or trusted server using the smart fob as an authentication tool, and while still connected to the PC use the stored value to pay for online products or services. This is particularly interesting for those that are uncomfortable using their credit card for online payments.

Parents can provide their teenagers with a smart fob loaded with a preset amount of cash and send them off to the mall or participating theatre and know that the money will be used as intended.

Teenagers are also among the most likely groups to pay on the Internet, however their inability to obtain credit cards and low online debit acceptance has historically made online payment difficult. This implies that a market for an alternative payment system targeted at teens exists and that web merchants must integrate new solutions if they want to target the teen market. Although teens can make purchases indirectly using a parent's credit cards, the buying experience is not the same due to the loss of independence for the teenager.

A prepaid or stored value apparatus such as the smart fob allows teens to shop on the Internet securely and without getting into debt. Although individually teenagers have limited income, together their income amounts to significant spending power. Therefore, there is a need in the market for a teen payment product that allows secure payments online.

Using an online shopping basket template, consumers can order groceries from the comfort of their home and collect them "ready to go" at the retail participating outlet, using their smart fob. Consumers enjoy increased convenience, faster shopping and quick checkout times. Retailers can quickly and easily take advantage of the order online & payment technology to speed transaction processing, increase revenue, and better understand customer buying behaviour.

Similar to the convenience store application, consumers can order rental movies online and collect them ready to go, using their smart fob. As transponders are used for inventory and anti-theft purposes in DVDs (digital versatile discs) and video tapes, the same data can be stored in the smart fob, allowing the consumer to just collect the rentals and leave without having to wait in a queue at the checkout.

Another application is using the smart fob for network access (logical access), remote mail and PC access. And to implement solutions to help organisations, establish more efficient business processes, address security concerns and gain a competitive advantage.

Users can connect to the corporate network or home PC from almost anywhere using one smart fob for roaming and another (stationary) for insertion in the desktop at work or home office computer. The smart fob inserted into the stationary PC is simultaneously connected directly to the DSL line or via an plug-in adapter. When the PC is switched off, the stationary smart fob draws it's energy from the telephone line, or from external power. When the roaming smart fob is plugged into an external Internet connected PC, the MAC (media access control) address of the stationary apparatus is called upon via the exchange secure server. This stationary smart fob switches on the PC and computing activity can begin. The stationary smart fob functions as a server and acts as a firewall with anti-virus software to protect the PC. The stationary smart fob, i.e. server, can have either a MAC address or a Uniform Resource Locator (URL) address.

Therefore, corporate computing resources can be reached from a home PC, an airport business centre, cyber-café or a kiosk computer allowing easy access to email, enterprise applications and data.

The smart fob can be used to reduce parent's anxiety by denying their children access to unsuitable websites, while permitting the children and teenagers access to the enjoyment and education value the Internet has to offer. The smart fob can be used to record and restrict all inbound and outbound Internet activity. By inserting the smart fob into the USB port of the home-PC, it enables the broadband, ISDN or analogue telephone connection, thus allowing access to the Internet. By mechanically disengaging the apparatus, the telephone line is disconnected, preventing access to the Internet. When children are allowed to surf on the Internet, data names concerning Internet sites or words put through search engines are compared with a library held in the memory of the smart fob. Therefore, children are independent and flexible to access the Internet without parental password control. Software updates can be automatic.

If a PC with DSL connection is left switched on, hackers or cyber-terrorists can potentially enter the PC as the broadband connection is constantly enabled. They are a real threat to the Internet and business information community. The smart fob can be used to disconnect the DSL line, by simply removing the device from the USB port. This prevents interference as well as preventing anyone from surfing the Internet from the user's PC. The physical DSL wire connection to the PC can remain, but access to the world wide web is only feasible when the USB apparatus is plugged back into one of the USB ports on the PC. Alternatively the USB apparatus can stay plugged in, but can be disengaged via a software code.

The smart fob can allow access to the worldwide web as a "free-Internet" service, making the ISP redundant. Also single applications can be stored on the secure server for selection by the client user.

In distress situations the user can use the smart fob to call for help, from the PC, from an icon (button) on the PC. Patient medical records can also be stored in the device.

When a user enters a hot zone area equipped with a Wi-Fi / 802.11 wireless local area network, such as a shopping mall, airport or cinemaplex, information, news or special offers can be sent to the smart fob. The consumer is alerted by visual and / or audible means that information relevant to his / her preferences (based on pre-registered data) have been received by the smart fob. Discounts can be sent in barcode format and redeemed at the participating merchant, by just displaying the barcode on the LCD (liquid crystal display) screen of the smart fob to a scanner at the checkout.

As the smart fob can receive messages in hot zone areas, it can be used to send a text message. (This, of course, would require at least a simple technique for entering text or sending stored, "standard" text messages.)

The smart fob can act as a content filter or for intrusion detection & prevention.

Music can be downloaded from the Internet using the smart fob as a storage device and for making electronic payment to a virtual music store. In the real world, the contactless function can be used to identify the consumer when he or she enters the high street store and to target the consumer with music of his or her preference at the listing booths.

Members can use the smart fob to communicate via the ISP or Trusted server with a club and to conduct transactions.

Law enforcement agencies cannot prevent the existence of adult content, but the concern is the exposure of children to such material on the Internet. The smart fob can be used to unscramble encoded content, operating in a similar fashion to a smart card in a television decoder box for cable TV viewing.

These are but a few of the potential uses for the smart fob of the present invention. One having ordinary skill in the art to which the present invention most nearly pertains will readily be able to implement these applications, based on the descriptions set forth herein.

Recap/Synopsis

Various features of the smart fob (e.g., compact personal token device) of the present invention are summarized and/or presented in the following numbered paragraphs.

¶1. A compact personal token apparatus, comprises:

a standard–compliant contact based interface; this interface complying to one or more of the following standard interfaces: USB (universal serial bus), IEEE1394 (Fire Wire), PCMCIA, Compact Flash, Multi Media, Memory Stick, Smart Media, Secure Digital (SD), mini SD, IBM Micro Drive, or any similar standard interface. These interfaces are all well known. ("Smart Media" refers to the Smart Media card, and "Secure Digital" refers to a Secure Digital (SD) card.)

This is a good place to mention the following. When a given standard or interface is specifically mentioned, it is typically intended to be an example of any other standard or interface that can perform substantially the same function as the standard(s) or interface(s) that are specifically mentioned. Many of these "other" standards and interfaces can be found in the GLOSSARY section hereinabove and/or are known in the industry and/or will evolve or be newly developed in the near future. The present invention should be interpreted to include all similar standards and interfaces, as appropriate to the context of the specific embodiments being discussed.

¶2. The compact personal token apparatus set forth in paragraph **¶1** further comprises:

a standard–compliant contactless / wireless interface; this interface complying to one or more of the following standard interfaces: RFID-contactless interface according to ISO 14443 and ISO 15693 as well as similar interfaces; Bluetooth compatible interface, WLAN 812.11, UWB, or any similar interface.

¶3. The compact personal token apparatus set forth in paragraph **¶1** further comprises:

a standard-compliant interface, releaseably coupleable to a host processing device, this being under the command of an operating system; an interface module providing the translation of standard-compliant contact based interface messages to ISO7816 compliant messages; the same interface module providing the translation of ISO7816 compliant messages to standard-compliant contact based interface messages; a dual interface processor having an ISO7816 compliant interface communicating through the interface module with the host processing device; the same dual interface processor communicating through its RFID-contactless interface like ISO 14443 and / or ISO 15693 or similar; the dual interface processor connected to an inductive antenna either being part of the PCB itself or en extra component inside the token.

¶4. The compact personal token apparatus set forth in paragraphs ¶1 or ¶2, further comprises:

a standard-compliant interface, releaseably coupleable to a host processing device, this being under the command of an operating system; an interface module providing the translation of standard-compliant contact based interface messages via a memory chip to Bluetooth /WLAN 812.11 device compatible compliant messages; the same interface module providing the translation of Bluetooth /WLAN 812.11 device compliant messages via a memory chip to standard-compliant contact based interface messages; a Bluetooth /WLAN 812.11 device having a Bluetooth/WLAN 812.11 compliant interface communicating through the interface module with the host processing device via a memory chip; the same Bluetooth /WLAN 812.11 device communicating through its Bluetooth /WLAN 812.11 compatible interface.

¶5. The compact personal token apparatus of paragraph ¶3, wherein:

the dual interface chip (processor) inside the personal token can be directly programmed by a software running on the host system using the interface processor without the need for an external contact based dual interface read/write device.

¶6. The apparatus of paragraph ¶5, wherein:

the software is web based, allowing for downloading information from the web directly into the dual interface processor memory (for example, event tickets) thus linking the virtual world to the real world.

¶7. The apparatus of paragraphs ¶5 or ¶6, wherein:

the downloaded information can be used in the real world by using the contactless RFID interface (e.g. public transport, e-payment and the like)

¶8. The apparatus of paragraphs ¶5 or ¶6, wherein:

the information stored in the personal token via the standard contact based interface is used for personal identification, secure network logon, access control, e-ticketing, e-payment and similar applications using either the standard compliant interface or the RFID-compliant interface.

¶9. The apparatus of paragraphs ¶5 or ¶6, wherein:

information received through the RFID- interface can be stored in the memory of the personal token and can then be provided to the host system via the standard interface, thus allowing a complete information exchange between the virtual world and the real world

¶10. The apparatus of paragraphs ¶3 or ¶4, wherein:

the contactless / wireless module is releaseably coupleable from the Interface module, thus providing a keyfob shape, easier to carry along.

¶11. The apparatus of paragraph ¶3, wherein:

the dual interface processor is mounted in a dual interface card complying to ISO 7810 and connected norms; the personal token providing physical contacts for the dual interface card; thus connected, the dual interface card can communicate with the host system through the interface module inside the personal token. Once the communication is done, the card can be released from the personal token and can be used then in the real world, just like described in paragraphs ¶5 to ¶9.

¶12. The compact personal token apparatus of paragraphs ¶1, ¶2 or ¶5, further comprises:

a flash memory or EEPROM device powered and addressed by the dual interface controller chip. The additional memory can be used for user authentication (storing digital signatures, certificates, key sets, finger-based biometric templates, usernames and passwords) and to run applications.

¶13. The compact personal token apparatus set forth in **¶1** further comprises:

a standard–compliant smart card contact interface complying to one or more of the following standard interfaces: ISO 7816, or any similar interface.

¶14. The compact personal token apparatus set forth in **¶2** further comprises:

a standard–compliant smart card contact interface complying to one or more of the following standard interfaces: ISO 7816, or any similar interface.

¶15. The compact personal token apparatus set forth in **¶1** further comprises:

a connection module, connecting the personal token apparatus to a host device such as PC, PDA, smart cellular phone or similar device, either directly or with the help of a standard reader device such as a memory card reader.

¶16. The compact personal token apparatus set forth in **¶1** further comprises:

a translation module, translating messages incoming from the contact based interface of claim 1, and translating messages to the host device from the personal token apparatus.

¶17. The compact personal token apparatus set forth in **¶1** further comprises:

a processor module, preparing messages to be sent by the contactless/wireless interface of ¶2, and interpreting messages received via the interface of ¶2.

¶18. The compact personal token apparatus set forth in **¶1** further comprises:

a triple interface (e.g., contact, contactless, USB) processor.

Additional Embodiments

The device (smart fob, USB key fob) can incorporate a SIM card or a SAM card.

It is not necessary that the device (smart fob, USB key fob) be equipped with all of the options for every application.

LEDs can be incorporated into the device (smart fob, USB key fob) to alert a user that certain functions are occurring.

The device (smart fob, USB key fob) can function as a mass memory device.

The device (smart fob, USB key fob) can function as a dongle for software license authentication.

The device (smart fob, USB key fob) can function as a token for providing network security. This embodiment could include a SIM card.

The device (smart fob, USB key fob) can function as a Smart Card for online-banking. This embodiment could include a SIM card.

The device (smart fob, USB key fob) can function as a Multi-Interface Reader-less Device to provide for physical and logical access control. This embodiment would include an RFID or NFC (Near Field Communication) antenna.

The device (smart fob, USB key fob) can function as a firewall to provide anti-virus protection. This embodiment would have a DSL plug-in socket and input-socket for external power.

In addition to the various formats of USB key fobs, it is contemplated to provide a docking station or hub that will accommodate at least two devices.

The flash memory could be integrated into the dual interface (DI) chip itself.

Additional Comments

Most memory based RFID chips or transponders have a unique modulation and communication protocol which influences the functionality and the type of antenna required for optimal operation. Because of the limitation on the size of the on-board EEPROM for such devices, the command set for Mifare, ISO 14443 A & B, ISO 15693, ISO 18000 or ISO 7816 resides on the ROM as well as being masked to the specific silicon device. The emergence of dual & triple interface micro-controllers opens up the possibility to integrate several communication protocols and modulation types onto a single device, by availing of the extensive memory capability of flash drive technology.

The advantage of loading the communication protocol and modulation type in software form to the flash memory eliminates the need to have several different type of chips with different antenna constructions for specific applications. True interoperability is achieved through software, resulting in higher volumes and yield for one particular controller.

Firewall Protection

Anti-Virus, - Worm, -Spam (and so forth) software normally resides on the home PC, slowing down it's functionality.

The device (smart fob, USB key fob) can comprise a 32 bit processor and 8 to 16 GB (GigaByte) memory capacity, and could be used as a server to protect the home PC from external intrusion. The device (smart fob, USB key fob) could have an IP (Internet Protocol) address, a socket for the broadband connection and a connection for external power. This USB server could be used to switch on the home PC from a remote location (using a MAC or IP address) in order to access files or to act as a protection guard from a constantly enabled DSL telephone line.

Downloading, Storing And Using Electronic Coupons ("E-Coupons").

The invention is a software application that uses the compact personal token apparatus referred to hereinabove as smart fob (again, this term is being used without prejudice to any trademark rights which may be claimed). The apparatus may also be referred to simply as "fob", or "personal device".

The basic concept allows registered consumers to visit a web site offering e-coupons ("coupon website") and

(1) down-load "e-coupons" to the fob at home or office, then

(2) take the fob with them to the retailer - grocery store or other participating merchant - and redeem the coupons for savings on their purchase.

In actual operation the consumer would, for example, log on to a participating manufacturer's web site (e.g., www.manufacturer's name.com) and be redirected to the coupon website (e.g., www. e-coupon website . com) when the consumer selects the "Download Coupon" function at the participating manufacturer's web site. This would be transparent to the consumer - the consumer would not realize they have left the merchant site.

This provides the ability for the consumer to:

1) load at home and store electronically, on a personal device - for example the smart fob or even a contactless or dual interface smart card (collectively, these various devices are simply referred to as the "fob") - a large number of coupons and then take that device into the real world with him.

2) at the checkout (e.g., merchant, retailer, grocery) the consumer purchases would be scanned into the register normally, the consumer would present his fob to the point of sale (POS) contactless reader terminal - software in the POS device ("merchant software") would compare the purchased items against the database of stored e-coupons on the fob or other smart object (i.e., contactless smart card) and decrement the value of the coupons off the fob and pass that savings amount to the register to deduct that savings amount from the total register receipt. The e-coupons registration info would also be passed on to the merchant POS system so that the merchant can bill the manufacturer for the coupon value he paid out. Redeemed coupon info remains stored on the fob - in background in a memory area not accessible or visible to the consumer, for later use. (see note 7a below)

3) In addition to value, the fob would also store the expiration date of each coupon. The consumer could elect to be notified of expiring coupons - all expiring, or only those meeting a preselected value (set "filters"). Expired coupons would be removed from the fob the next time the consumer logs onto the home computer. (Unused coupon information would remain on the fob in the same secure inaccessible memory area - (see note 7b below)

4) The consumer side of the software ("home software") could also have a grocery list function, that could be printed out at home.

5) The home software would also allow the consumer to see the total value of coupons stored on the fob, total by product or category and a total of the redeemed coupons or actual savings.

6) The home software would allow the consumer to store a credit card and/or debit card on the fob to pay for the purchase if they choose not to pay with cash.

7a) The home software would also send purchase data - redeemed & expired coupon info back to the coupon website at the time the consumer does a new coupon download. This feature correlates specific coupon purchases with an identifiable consumer.

7b) The coupon website could also offer a fee based service to manufacturers or retailers to alert them (or even their competitor) that a predetermined time has passed since the consumer last used a coupon to purchase the specific item. (Unused coupon info may also be of some value to a manufacturer.) The merchant would then have the option of emailing the consumer another coupon for the product to stimulate a new buying decision, a competitor may want to send a coupon to the customer to attempt to change brand preference. These customer notification features could be permission-based allowing the consumer to opt-out.

The above is summarized in the following "flowchart".

======================

user plugs fob (personal device) into computer

user logs onto to manufacturer website
  redirected to coupon website

user downloads e-coupons onto fob

home software checks for expired or expiring coupons
  user notified of expiring coupons
  expired coupons deleted from fob
  (optional) coupon website notifies manufacturer/retailer/competitor of expired coupons.

home software displays total value of stored coupons, savings, etc.

home software uploads purchase data to coupon website (optional) home software has a grocery list function

(optional) home software can store user's credit card info on fob

user take fob to merchant, make purchase(s), redeem coupons

- merchant scans purchases
- merchant software compares coupons with purchases
- merchant software writes to fob, decrements coupons (or marks as used)
- (optional) merchant loads premiums onto user's fob
- merchant bills manufacturer

user returns home and plugs fob into computer for next session

=====================

Some of the Advantages of the Invention

Print at home coupons via the internet are available to consumers today. However, the consumer still has to remember to take them with him to the grocery, retail, fast food store. Merchants and manufacturers are experiencing fraud - counterfeit coupons or value changed. This has limited the growth of this type of couponing. The present invention would eliminate or substantially reduce the fraud aspect of at home couponing - all coupons are stored electronically in a secure memory cell.

Another problem solved by the invention is that sometimes cashiers just accept a plurality (hand full) of coupons from the shopper and deduct all the coupons - even if the item was not purchased. The present invention would eliminate this problem of redeemed coupons without product purchase.

The invention provides for effective management of manufacturers coupons - eliminate lost or forgotten coupons - maximize savings. Grocery or manufacturer can pass savings on to consumers.

Additional embodiments

Rather than using the smart fob, or other fobs discussed hereinabove, the customer can plug a standard USB memory (stick) device into his home/office computer - download the home software, then down load coupons to the USB memory device and then at the participating grocery store or retail merchant plug the USB memory device into a POS device (cash register, kiosk etc) equipped with a USB receptacle connector to exchange stored coupons for savings. With the pure USB memory stick device there is no need to use the ISO7816 smart card standard interface, or the ISO 14443 RFID protocol - just use standard USB communication protocol. (The smart fob embodiment of the invention communicates using ISO7816 when the consumer has it plugged into his PC (USB to 7816 conversion) but at the grocery or retail outlet the communication is contactless using the ISO 14443 type A or B or Mifare standards.)

The merchant can upload data ("premiums") to the consumers fob (or USB memory device) at the POS (point of sale) terminal. This could be in the form of additional coupons for in store promotions, loyalty points or even music. Some of this digital content could be encrypted for limited time use or conditional access.

Optionally, all coupons are encrypted as a security feature reducing or eliminating the likelihood that coupon values could be counterfeited or altered in any way.

The invention has been illustrated and described in a manner that should be considered as exemplary rather than restrictive in character - it being understood that only preferred embodiments have been shown and described, and that all changes and modifications that come within the spirit of the invention are desired to be protected. Undoubtedly, many other "variations" on the techniques set forth hereinabove will occur to one having ordinary skill in the art to which the present invention most nearly pertains, and such variations are intended to be within the scope of the invention, as disclosed herein.

For example, a fob-style device designed for the PC environment, which plugs into the USB port of a computer, with an antenna coil in the device that enables the contactless part of a separate contactless smart card to communicate with contactless readers.

For example, a triple interface chip incorporating a range of highly secure smart card controllers - ISO 7816 contact interface, ISO 14443A contactless Interface and USB 1.1 (or 2.0) Interface. Additionally, incorporating a fourth interface for connecting directly to the Internet, such as via a DSL line.

For example, telephone handsets (also known as "cell phones" or "mobile phones") are providing slots for flash memory cards, such as SD (Secure Digital) and MMC (MultiMediaCard) cards, mainly for storing pictures. The present invention could be embodied in the form of a flash memory card such as a "smart" SD card" (comparable to the aforementioned "smart fob"), which could also include an antenna and tamper-resistant area which can be inserted into handsets for performing various of the e-commerce and other applications mentioned above.

For example, a smart SD card using a contact-based standard interface (e.g., SD card format) to load data to and from the card with the help of a card reader hooked to a PC or incorporated into a PDA, cell phone, etc, and which uses a contactless standard interface to use the stored data in the real world. Additional memory can be used to securely store customer information and data

For example, with such a smart SD card, adding RFID to an apparatus (appliance) having an SD or miniSD memory card slot, such as a cell phone, PDA, laptop, digital camera, personal video player, MP3 player, etc.

For example, incorporating the latest technologies into the smart SD card (or with the smart fob described hereinabove), such as non-volatile FeRAM (ferroelectric RAM), which enables high-speed data writing, five times faster than conventional EEPROM-based smart cards. The large-capacity flash memory in the smart SD Card can be used as an extra storage area for the smart card module and the stored data is protected by cipher technology.

CLAIMS

What is claimed is:

1. A compact personal token apparatus, comprising:

a connection module;

a translation module;

a processor module; and

an input/output module.

2. The compact personal token apparatus of claim 1, wherein:

the connection module is for interfacing the personal token apparatus with a an Internet-capable appliance; and

the interface is selected from the group consisting of USB, FireWire, IR, Bluetooth, standard serial port, WLAN.

3. The compact personal token apparatus of claim 1, wherein:

the connection module is for interfacing the personal token apparatus with a an Internet-capable appliance; and

the Internet-capable appliance comprises a device selected from the group consisting of personal computer (PC), laptop, PDA, MP3 player and cellphone.

4. The compact personal token apparatus of claim 1, wherein:

the translation module moves signals between a USB interface and a smart card interface.

5. The compact personal token apparatus of claim 4, wherein:

the smart card interface is selected from the group consisting of ISO 7816, ISO 14443 and ISO 15693.

6. The compact personal token apparatus of claim 1, wherein:

the processor module comprises a dual interface (DI) chip.

7. The compact personal token apparatus of claim 1, wherein:
the processor module incorporates the translation module.

8. The compact personal token apparatus of claim 1, wherein:
the output module comprises an RF antenna and a modulator.

9. The compact personal token apparatus of claim 1, further comprising:
flash memory.

10. The compact personal token apparatus of claim 1, wherein:
the translation module moves signals between a USB interface and a wireless interface.

11. The compact personal token apparatus of claim 1, wherein:
the translation module is incorporated in the processor module to that the device can go directly from USB to wireless without being limited by smart card software architecture limitations.

12. The compact personal token apparatus of claim 1, wherein:
the modules are embodied in the form of an apparatus having the general physical configuration of a conventional USB memory fob.

13. The compact personal token apparatus of claim 12, wherein the fob comprises;
a first physical module containing the input module and the translation module; and
a second physical module containing the processor module and the output module.

14. The compact personal token apparatus of claim 1, wherein:
the output module comprises contacts for interfacing with a smart card.

15. The compact personal token apparatus of claim 1, wherein:

the fob is capable of interfacing with the Internet and emulating a smart card.

16. The compact personal token apparatus of claim 1, wherein:

the connection module is for interfacing the personal token apparatus with an Internet-capable appliance; and further comprising:

an input module is for connecting to the Internet; and

the apparatus incorporates firewall functionality to protect the Internet-capable applicance.

17. The compact personal token apparatus of claim 1, further comprising:

interfaces for ISO contact, contactless, USB and DSL.

18. The compact personal token apparatus of claim 1, further comprising:

an LCD screen.

19. The compact personal token apparatus of claim 1, further comprising:

at least one switch.

20. The compact personal token apparatus of claim 1, further comprising:

at least one LED.

21. A compact personal token apparatus comprising:

a standard–compliant contact based interface, the contact based interface complying to at least one standard interface selected from the group consisting of USB, IEEE 1394, PCMCIA, Compact Flash, Multi Media, Memory Stick, Smart Media, Secure Digital, mini SD, IBM Micro Drive, and any similar standard interface.

22. The compact personal token apparatus of claim 21, further comprising:

a standard–compliant contactless/wireless interface; the contactless/wireless interface complying to one or more of the following standard interfaces: RFID-contactless interface according to ISO 14443 and ISO 15693 as well as similar interfaces, Bluetooth compatible interface, WLAN 812.11, UWB, and any similar interface.

23. The compact personal token apparatus of claim 22, further comprising:

a standard-compliant interface releaseably coupleable to a host processing device, this being under the command of an operating system;

an interface module providing translation of standard-compliant contact based interface messages via a memory chip to Bluetooth /WLAN 812.11 device compatible compliant messages, and providing the translation of Bluetooth /WLAN 812.11 device compliant messages via a memory chip to standard-compliant contact based interface messages; and

a Bluetooth /WLAN 812.11 device having a Bluetooth/WLAN 812.11 compliant interface communicating through the interface module with the host processing device via a memory chip; the same Bluetooth /WLAN 812.11 device communicating through its Bluetooth /WLAN 812.11 compatible interface.

24. The compact personal token apparatus of claim 23, wherein:

the contactless / wireless module is releaseably coupleable from the Interface module.

25. The compact personal token apparatus of claim 22, further comprising:

a processor module; and

additional memory selected from the group consisting of flash memory and EEPROM device powered and addressed by the processor module;

wherein the additional memory can be used for user authentication and to run applications.

26. The compact personal token apparatus of claim 22, further comprising:

a standard–compliant smart card contact interface complying to ISO 7816, or any similar interface.

27. The compact personal token apparatus of claim 22, further comprising:

a processor module, preparing messages to be sent by the contactless/wireless interface of and interpreting messages received via the interface.

28. The compact personal token apparatus of claim 21, further comprising:

a standard-compliant interface releaseably coupleable to a host processing device, this being under the command of an operating system;

an interface module providing translation of standard-compliant contact based interface messages to ISO 7816 compliant messages and providing the translation of ISO 7816 compliant messages to standard-compliant contact based interface messages;

a dual interface processor having an ISO7816 compliant interface communicating through the interface module with the host processing device, the dual interface processor communicating through an RFID-contactless interface and connected to an inductive antenna.

29. The compact personal token apparatus of claim 28, wherein:

the contactless / wireless module is releaseably coupleable from the Interface module.

30. The compact personal token apparatus of claim 28, wherein:

the dual interface processor is mounted in a dual interface card complying to ISO 7810 or a 7816 compliant SIM module and connected norms;

the compact personal token apparatus provides physical contacts for the dual interface card, or a 7816 compliant form factor; and

when connected, the dual interface or SIM card can communicate with the host processing device through the interface module inside the personal token and, once the communication is done, the card can be released from the personal token and can be used then in the real world.

31. The compact personal token apparatus of claim 28, wherein:

the dual interface chip (processor) inside the personal token can be directly programmed by a software running on the host system using the interface processor without the need for an external contact based dual interface read/write device.

32. The compact personal token apparatus of claim 31, wherein:

the downloaded information can be used in the real world by using the contactless RFID interface.

33. The compact personal token apparatus of claim 31, wherein:

the software is web based, allowing for downloading information from the web directly into the dual interface processor memory (for example, event tickets) thus linking the virtual world to the real world.

34. The compact personal token apparatus of claim 33, wherein:

the downloaded information can be used in the real world by using the contactless RFID interface.

35. The compact personal token apparatus of claim 33, wherein:

the information stored in the personal token via the standard contact based interface is used for personal identification, secure network logon, access control, e-ticketing, e-payment and similar applications using either the standard compliant interface or the RFID-compliant interface.

36. The compact personal token apparatus of claim 33, wherein:

information received through the RFID- interface can be stored in the memory of the personal token and can then be provided to the host processing device via the standard interface, thus allowing a complete information exchange between the virtual world and the real world.

37. The compact personal token apparatus of claim 31, wherein:

the information stored in the personal token via the standard contact based interface is used for personal identification, secure network logon, access control, e-ticketing, e-payment and similar applications using either the standard compliant interface or the RFID-compliant interface.

38. The compact personal token apparatus of claim 31, wherein:

information received through the RFID- interface can be stored in the memory of the personal token and can then be provided to the host processing device via the standard interface, thus allowing a complete information exchange between the virtual world and the real world.

39. The compact personal token apparatus of claim 31, further comprising:

additional memory selected from the group consisting of flash memory and EEPROM device powered and addressed by the processor module;

wherein the additional memory can be used for user authentication and to run applications.

40. The compact personal token apparatus of claim 21, further comprising:

a standard-compliant interface releaseably coupleable to a host processing device, this being under the command of an operating system;

an interface module providing translation of standard-compliant contact based interface messages via a memory chip to Bluetooth /WLAN 812.11 device compatible compliant messages, and providing the translation of Bluetooth /WLAN 812.11 device compliant messages via a memory chip to standard-compliant contact based interface messages; and

a Bluetooth /WLAN 812.11 device having a Bluetooth/WLAN 812.11 compliant interface communicating through the interface module with the host processing device via a memory chip; the same Bluetooth /WLAN 812.11 device communicating through its Bluetooth /WLAN 812.11 compatible interface.

41. The compact personal token apparatus of claim 21, further comprising:

a processor module; and

additional memory selected from the group consisting of flash memory and EEPROM device powered and addressed by the processor module;

wherein the additional memory can be used for user authentication and to run applications.

42. The compact personal token apparatus of claim 21, further comprising:

a standard–compliant smart card contact interface complying to ISO 7816, or any similar interface.

43. The compact personal token apparatus of claim 21, further comprising:

a connection module, connecting the personal token apparatus to a host device such as PC, PDA, smart cellular phone or similar device, either directly or with the help of a standard reader device such as a memory card reader.

44. The compact personal token apparatus of claim 21, further comprising:

a standard-compliant interface releaseably coupleable to a host processing device, this being under the command of an operating system; and

a translation module, translating messages incoming from the contact based interface, and translating messages to the host device from the personal token apparatus.

45. The compact personal token apparatus of claim 21, further comprising:

a triple interface (e.g., contact, contactless, USB) processor.

46. Method of interacting wirelessly, comprising:

providing a device;

interfacing the device with a an Internet-capable appliance; and

providing a smart card interface in the device.

47. Method, according to claim 46, wherein:

the interface with the Internet-capable appliance is selected from the group consisting of USB, FireWire, IR, Bluetooth, standard serial port, WLAN.

48. Method, according to claim 46, wherein:

the Internet-capable appliance comprises a device selected from the group consisting of personal computer (PC), laptop, PDA, MP3 player and cell phone.

49. Method, according to claim 46, wherein:

the smart card interface is selected from the group consisting of ISO 7816, ISO 14443 and ISO 15693.

50. Method, according to claim 46, wherein:

the device is modular in construction.

51. Method, according to claim 46, wherein:

the device performs a firewall functionality to protect the Internet-capable applicance.

52. Method, according to claim 46, wherein:

the device incorporates interfaces for ISO contact, contactless, USB and DSL.

ABSTRACT

A compact personal token apparatus, suitably resembling a conventional USB memory fob in size, shape, and form which can be plugged into a PC and interfaced with the virtual world of the Internet. The apparatus is capable of loading and storing information from the Internet, via the PC to its flash memory or EEPROM and then using the stored information or value via its wireless interface in the real world. The apparatus is capable of implementing an auto-run application, when inserted into a personal computer. The apparatus is capable of exchanging information with other devices having compatible interfaces. The apparatus can also function as a firewall when plugged between an Internet connection and a PC.

FIG 1A

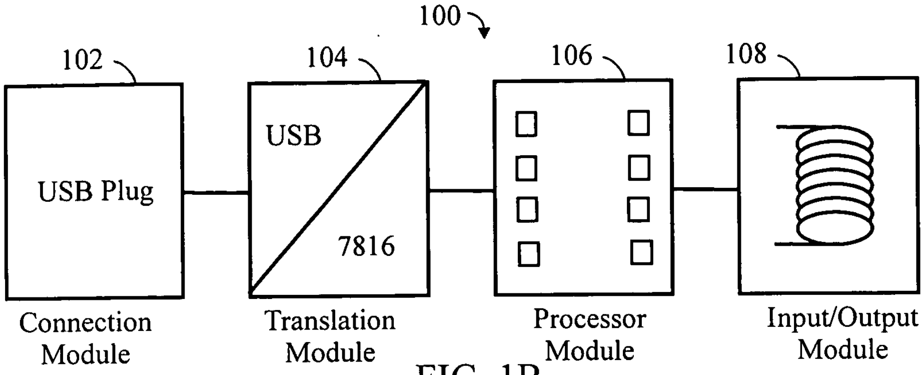


FIG. 1B

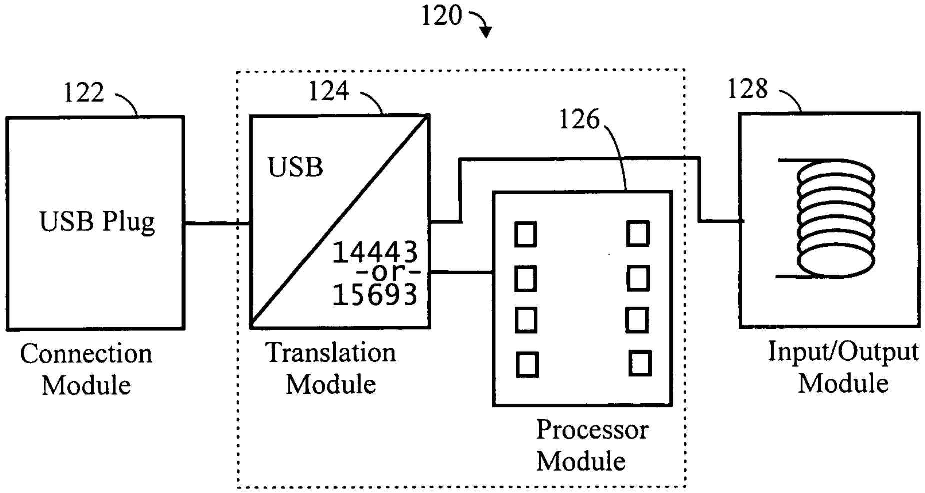


FIG 1C

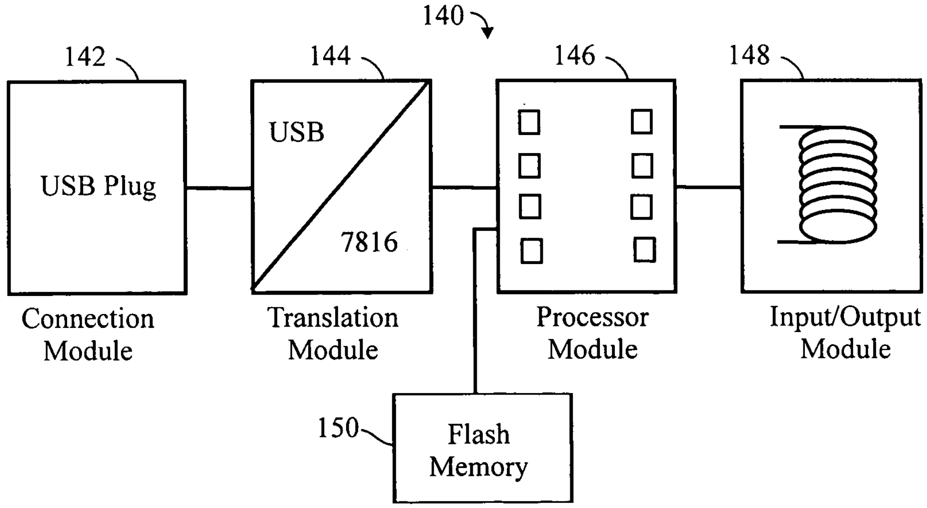


FIG. 2A

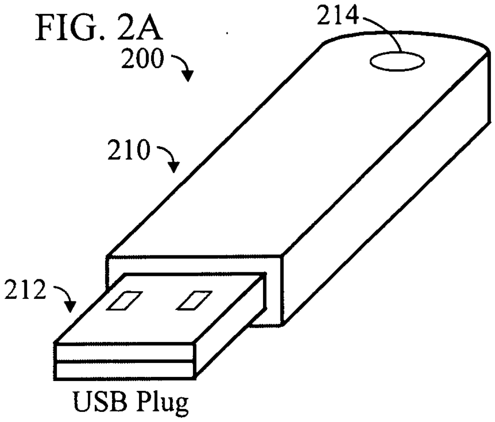


FIG. 2B

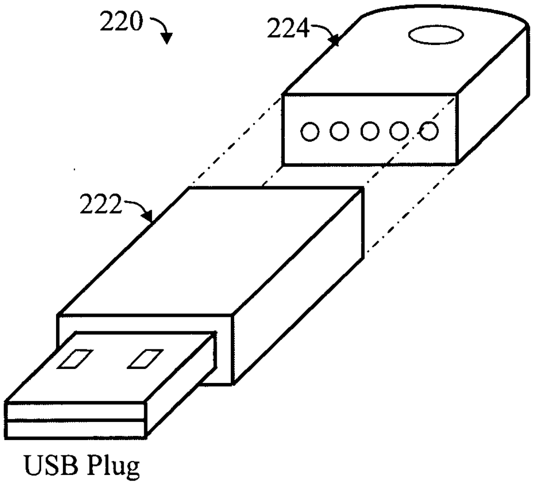


FIG. 3A

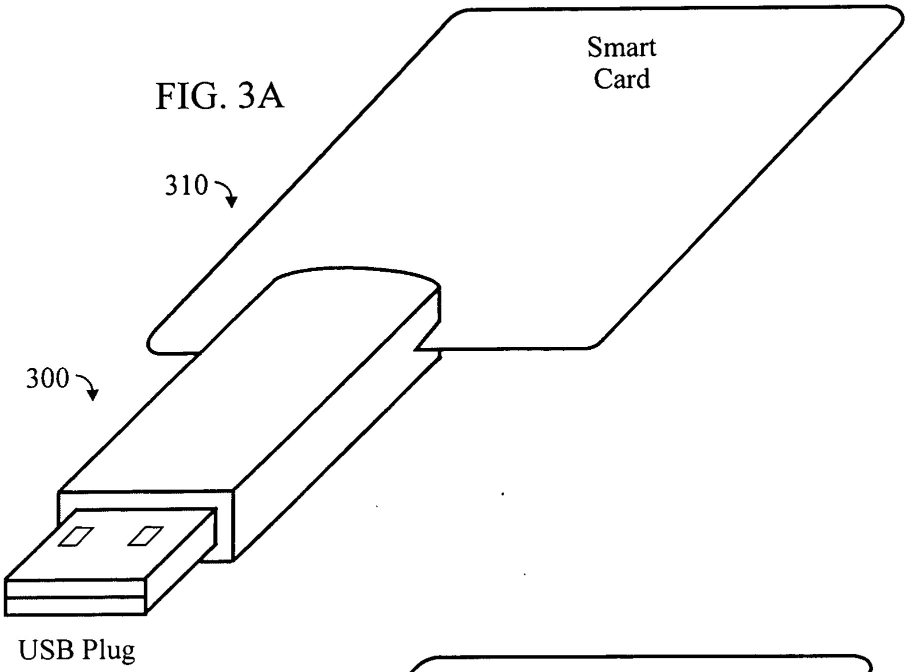

Smart
Card
310
300
USB Plug

FIG. 3B

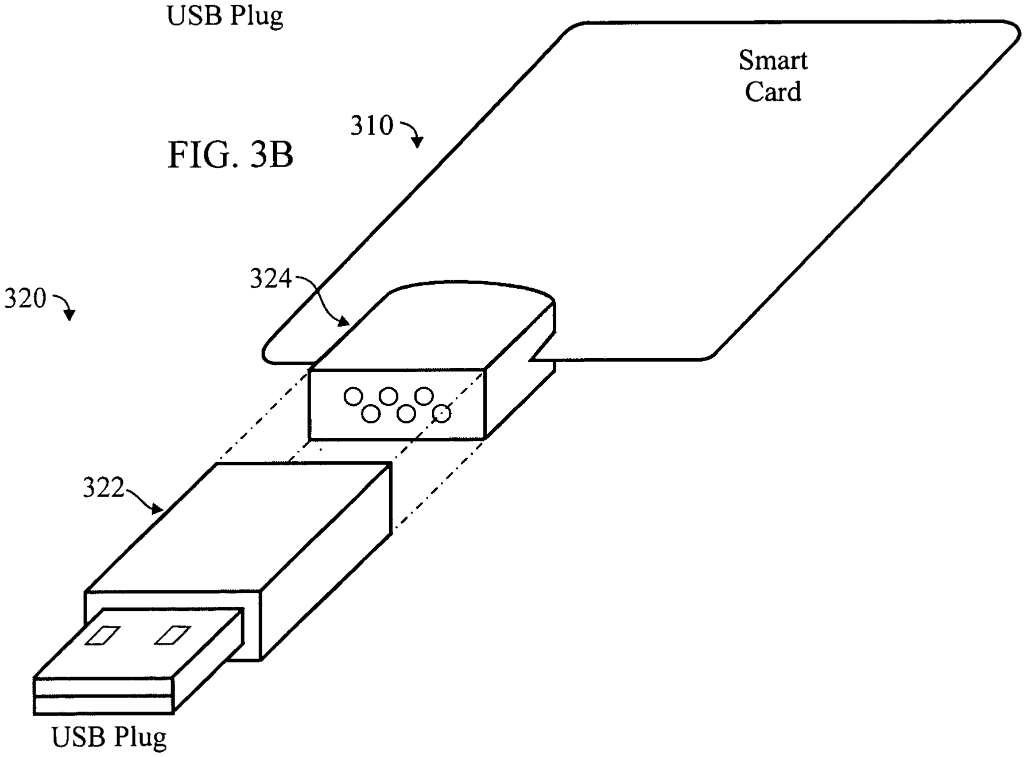
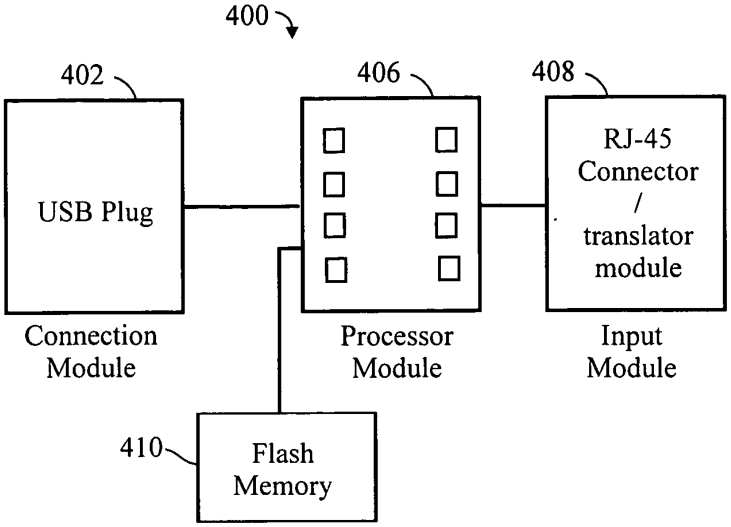
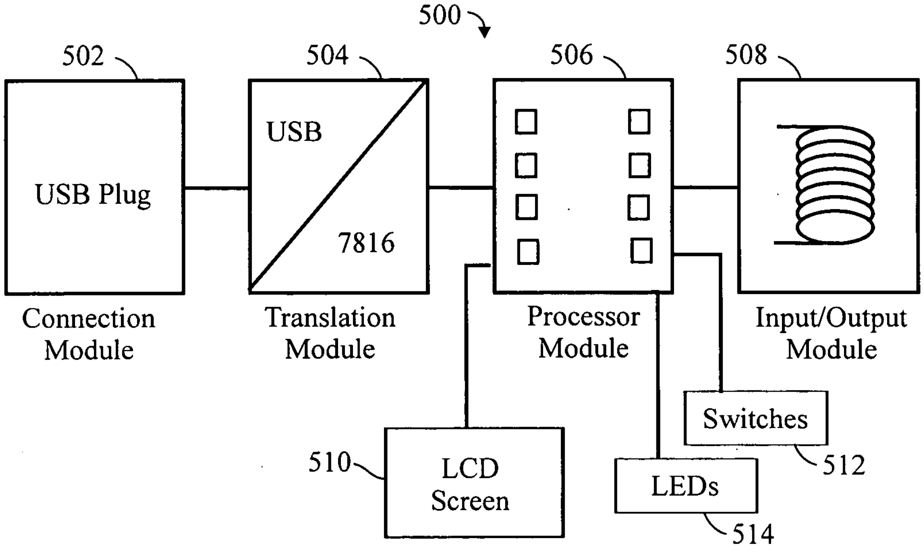

Smart
Card
310
320
324
322
USB Plug

FIG 4



400
402
406
408
USB Plug
RJ-45 Connector / translator module
Connection Module
Processor Module
Input Module
410
Flash Memory

FIG 5



500
502
504
506
508
USB Plug
USB
7816
Connection Module
Translation Module
Processor Module
Input/Output Module
Switches
512
510
LCD Screen
LEDs
514

Attorney Docket: Ryan C-4

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY

Title: MULTI-INTERFACE COMPACT PERSONAL TOKEN APPARATUS AND METHODS OF USE
Inventor(s): Ryan, et al.
Serial Number: -tbd-
Filing Date: -herewith-

===

As a below inventor, I hereby declare that; My residence, post office address and citizenship are as stated below next to my name; that I verily believe that I am an original, **JOINT** inventor of the subject matter which is claimed and for which a patent is sought on the above-referenced invention.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above; that the above-identified specification contains a complete and accurate description of the subject matter which is claimed and for which a patent is sought.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, CFR §1.56(a).

I hereby claim benefit under Title 35, United States Code, §120 of any United States applications that are listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in those prior applications in the manner provided by the first paragraph of Title 35, United States Code §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations §1.56(a) which occurred between the filing date of the prior applications and the filing date of this application. I further claim benefit under Title 35 United States Code, §119 of any international patent applications listed below:

USSN 60/520,698 filed 11/17/2003 by Ryan, et al.
USSN 60/562,204 filed 4/14/2004 by Comiskey, et al.
USSN 60/602,595 filed 8/18/2004 by Finn

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following agent(s) / attorney(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith:

GERALD E. LINDEN, Registration No. 30,282
DWIGHT A. STAUFFER, Registration No. 47,963

Declaration of Ryan, et al. page 1/2

Declaration of Ryan, et al. page 2/2

Title: MULTI-INTERFACE COMPACT PERSONAL TOKEN APPARATUS AND
METHODS OF USE
Inventor(s): Ryan, et al.

==

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

________________ ________ US
Dennis J. Ryan Date Citizenship
2739 E Virgo Place Chandler, AZ 85249
Residence and Post Office Address

________________ ________ Ireland
David Finn Date Citizenship
Lower Churchfield, Tourmakeady County, Mayo, Ireland
Residence and Post Office Address

________________ ________ US
Patrick R. Comiskey Date Citizenship
2408 Edgerton Road University Heights, Ohio 44118
Residence and Post Office Address

________________ ________ Germany
Norbert Knapich Date Citizenship
Mangmuehlerweg 5, Rosshaupten 87672, Germany
Residence and Post Office Address

PATENT APPLICATION FEE DETERMINATION RECORD

Effective December 8, 2004

10990296

CLAIMS AS FILED - PART I

	(Column 1)	(Column 2)
TOTAL CLAIMS	52	
FOR	NUMBER FILED	NUMBER EXTRA
TOTAL CHARGEABLE CLAIMS	52 minus 20=	* 32
INDEPENDENT CLAIMS	3 minus 3 =	*
MULTIPLE DEPENDENT CLAIM PRESENT		□

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

SMALL ENTITY TYPE □ OR OTHER THAN SMALL ENTITY

RATE	FEE		RATE	FEE
BASIC FEE	395	OR	BASIC FEE	790
X$ 25=	800	OR	X$50=	
X100=		OR	X200=	
+180=		OR	+360=	
TOTAL	1195	OR	TOTAL	

CLAIMS AS AMENDED - PART II

AMENDMENT A

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				□

SMALL ENTITY OR OTHER THAN SMALL ENTITY

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 25=		OR	X$50=	
X100=		OR	X200=	
+180=		OR	+360=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT B

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				□

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 25=		OR	X$50=	
X100=		OR	X200=	
+180=		OR	+360=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT C

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				□

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 25=		OR	X$50=	
X100=		OR	X200=	
+180=		OR	+360=	

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371 (c) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
10/990,296	11/16/2004	Dennis J. Ryan	Ryan C-4

CONFIRMATION NO. 2050

FORMALITIES LETTER

OC000000014782349

Gerald E. Linden
12925 La Rochelle Cr.
Palm Beach Gardens, FL 33410

Date Mailed: 12/16/2004

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The statutory basic filing fee is missing.
  Applicant must submit $ **395** *to complete the basic filing fee for a small entity.*
- The oath or declaration is unsigned.
- To avoid abandonment, a late filing fee or oath or declaration surcharge as set forth in 37 CFR 1.16(e) of $65 for a small entity in compliance with 37 CFR 1.27, must be submitted with the missing items identified in this letter.

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- Additional claim fees of **$800** as a small entity, including any required multiple dependent claim fee, are required. Applicant must submit the additional claim fees or cancel the additional claims for which fees are due.

SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is **$1260** for a Small Entity

- **$395** Statutory basic filing fee.
- **$65** Late oath or declaration Surcharge.

- Total additional claim fee(s) for this application is **$800**

  - **$800** for **32** total claims over 20.

Replies should be mailed to:

Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

A copy of this notice <u>MUST</u> be returned with the reply.

Customer Service Center
Initial Patent Examination Division (703) 308-1202

PART 3 - OFFICE COPY

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NUMBER	FILING OR 371 (c) DATE	FIRST NAMED APPLICANT	ATTORNEY DOCKET NUMBER
10/990,296	11/16/2004	Dennis J. Ryan	Ryan C-4

CONFIRMATION NO. 2050

Gerald E. Linden
12925 La Rochelle Cr.
Palm Beach Gardens, FL 33410

FORMALITIES LETTER

OC000000014782349

Date Mailed: 12/16/2004

NOTICE TO FILE MISSING PARTS OF NONPROVISIONAL APPLICATION

FILED UNDER 37 CFR 1.53(b)

Filing Date Granted

Items Required To Avoid Abandonment:

An application number and filing date have been accorded to this application. The item(s) indicated below, however, are missing. Applicant is given **TWO MONTHS** from the date of this Notice within which to file all required items and pay any fees required below to avoid abandonment. Extensions of time may be obtained by filing a petition accompanied by the extension fee under the provisions of 37 CFR 1.136(a).

- The statutory basic filing fee is missing.
  Applicant must submit $ **395** *to complete the basic filing fee for a small entity.*
- The oath or declaration is unsigned.
- To avoid abandonment, a late filing fee or oath or declaration surcharge as set forth in 37 CFR 1.16(e) of $65 for a small entity in compliance with 37 CFR 1.27, must be submitted with the missing items identified in this letter.

The applicant needs to satisfy supplemental fees problems indicated below.

The required item(s) identified below must be timely submitted to avoid abandonment:

- Additional claim fees of **$800** as a small entity, including any required multiple dependent claim fee, are required. Applicant must submit the additional claim fees or cancel the additional claims for which fees are due.

SUMMARY OF FEES DUE:

Total additional fee(s) required for this application is **$1260** for a Small Entity

- **$395** Statutory basic filing fee.
- **$65** Late oath or declaration Surcharge.

- Total additional claim fee(s) for this application is **$800**
  - **$800** for **32** total claims over 20.

Replies should be mailed to: Mail Stop Missing Parts
Commissioner for Patents
P.O. Box 1450
Alexandria VA 22313-1450

A copy of this notice <u>MUST</u> be returned with the reply.

Customer Service Center
Initial Patent Examination Division (703) 308-1202

PART 1 - ATTORNEY/APPLICANT COPY

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Title: MULTI-INTERFACE COMPACT PERSONAL TOKEN APPARATUS AND METHODS OF USE
Inventor(s): RYAN, et al.
Serial Number: 10/990,296
Filing Date: 11/16/2004

TRANSMITTAL

To: MAIL STOP - Missing Parts
COMMISSIONER FOR PATENTS
P.O. BOX 1450
ALEXANDRIA, VA 22313-1450

Enclosed herewith for filing is:

- NOTICE TO FILE MISSING PARTS ...
- DECLARATIONs < ***two*** signed by the inventors, each is ***two*** pages
  - **Ryan** and **Comiskey**, signed 11/22/2004 and 12/31/2004
  - **Finn** and **Knapich**, signed 12/30/2004
- Filing Fee (**395**) and excess claims fee (**800**) and Surcharge (**65**)

Total fees enclosed herewith = **$1260** Charge any shortfall to Dep. Acct. 12-1445.

Future Correspondence
Please direct all future correspondence in this matter to:
GERALD E. LINDEN
12925 LA ROCHELLE CR.
PALM BEACH GARDENS, FL 33410

Certificate of Mailing
I, the undersigned, hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope with sufficient postage addressed to Commissioner for Patents, Alexandria, VA 22313, on the date indicated below.

For the applicant,

Gerald E. Linden 1/18/05
Gerald E. Linden 30,282 date
(561) 694-2094

Attorney Docket: Ryan C-4

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY

Title: MULTI-INTERFACE COMPACT PERSONAL TOKEN APPARATUS AND
METHODS OF USE
Inventor(s): Ryan, et al.
Serial Number: -tbd-
Filing Date: Nov. 16, 2004

As a below inventor, I hereby declare that; My residence, post office address and citizenship are as stated below next to my name; that I verily believe that I am an original, **JOINT** inventor of the subject matter which is claimed and for which a patent is sought on the above-referenced invention.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above; that the above-identified specification contains a complete and accurate description of the subject matter which is claimed and for which a patent is sought.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, CFR §1.56(a).

I hereby claim benefit under Title 35, United States Code, §120 of any United States applications that are listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in those prior applications in the manner provided by the first paragraph of Title 35, United States Code §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations §1.56(a) which occurred between the filing date of the prior applications and the filing date of this application. I further claim benefit under Title 35 United States Code, §119 of any international patent applications listed below:

USSN 60/520,698 filed 11/17/2003 by Ryan, et al.
USSN 60/562,204 filed 4/14/2004 by Comiskey, et al.
USSN 60/602,595 filed 8/18/2004 by Finn

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following agent(s) / attorney(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith:

GERALD E. LINDEN, Registration No. 30,282
DWIGHT A. STAUFFER, Registration No. 47,963

Declaration of Ryan, et al. page 2/2

Title: MULTI-INTERFACE COMPACT PERSONAL TOKEN APPARATUS AND METHODS OF USE
Inventor(s): Ryan, et al.

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

11/22/04 US .
Dennis J. Ryan Date Citizenship
2739 E Virgo Place Chandler, AZ 85249
Residence and Post Office Address

Ireland .
David Finn Date Citizenship
Lower Churchfield, Tourmakeady County, Mayo, Ireland
Residence and Post Office Address

12-31-04 US .
Patrick R. Comiskey Date Citizenship
2408 Edgerton Road University Heights, Ohio 44118
Residence and Post Office Address

Germany .
Norbert Knapich Date Citizenship
Mangmuehlerweg 5, Rosshaupten 87672, Germany
Residence and Post Office Address

Attorney Docket: Ryan C-4

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

COMBINED DECLARATION FOR PATENT APPLICATION AND POWER OF ATTORNEY

Title: MULTI-INTERFACE COMPACT PERSONAL TOKEN APPARATUS AND METHODS OF USE
Inventor(s): Ryan, et al.
Serial Number: 10/990,296
Filing Date: Nov. 16, 2004

As a below inventor, I hereby declare that; My residence, post office address and citizenship are as stated below next to my name; that I verily believe that I am an original, **JOINT** inventor of the subject matter which is claimed and for which a patent is sought on the above-referenced invention.

I hereby state that I have reviewed and understand the contents of the above-identified specification, including the claims, as amended by any amendment referred to above; that the above-identified specification contains a complete and accurate description of the subject matter which is claimed and for which a patent is sought.

I acknowledge the duty to disclose information which is material to the examination of this application in accordance with Title 37, CFR §1.56(a).

I hereby claim benefit under Title 35, United States Code, §120 of any United States applications that are listed below and, insofar as the subject matter of each of the claims of this application is not disclosed in those prior applications in the manner provided by the first paragraph of Title 35, United States Code §112, I acknowledge the duty to disclose material information as defined in Title 37, Code of Federal Regulations §1.56(a) which occurred between the filing date of the prior applications and the filing date of this application. I further claim benefit under Title 35 United States Code, §119 of any international patent applications listed below:

USSN 60/520,698 filed 11/17/2003 by Ryan, et al.
USSN 60/562,204 filed 4/14/2004 by Comiskey, et al.
USSN 60/602,595 filed 8/18/2004 by Finn

POWER OF ATTORNEY: As a named inventor, I hereby appoint the following agent(s) / attorney(s) to prosecute this application and transact all business in the Patent and Trademark Office connected therewith:

GERALD E. LINDEN, Registration No. 30,282
DWIGHT A. STAUFFER, Registration No. 47,963

Declaration of Ryan, et al. page 2/2

Title: MULTI-INTERFACE COMPACT PERSONAL TOKEN APPARATUS AND METHODS OF USE
Inventor(s): Ryan, et al.
Serial Number: 10/990,296
Filing Date: Nov. 16, 2004

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

__________ ______ US
Dennis J. Ryan Date Citizenship
2739 E Virgo Place Chandler, AZ 85249
Residence and Post Office Address

David Finn 30.12.04 Ireland
David Finn Date Citizenship
Lower Churchfield, Tourmakeady County, Mayo, Ireland
Residence and Post Office Address

__________ ______ US
Patrick R. Comiskey Date Citizenship
2408 Edgerton Road University Heights, Ohio 44118
Residence and Post Office Address

30.12.04 Germany
Norbert Knapich Date Citizenship
Mangmuehlerweg 5, Rosshaupten 87672, Germany
Residence and Post Office Address

IFW

Atty Docket: Ryan-C4

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Title: MULTI-INTERFACE COMPACT PERSONAL TOKEN APPARATUS AND METHODS OF USE

Inventor(s): RYAN, et al.

Serial No: 10/990,296

Filing Date: 11/16/2004

CHANGE OF CONTACT PERSON (and Correspondence Address)

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

I (Gerald E. Linden) am currently the attorney of record (named on the DECLARATION, as filed).

Dwight A. Stauffer (Reg # 47963) has been appointed with Power of Attorney.

Dwight A. Stauffer is a practitioner associated with Customer Number # 37053. Phone (216) 381-6599

Correspondence Address
Please change the correspondence address for the above-identified application to:
Customer Number # 37053
Dwight A. Stauffer
1006 Montford Rd.
Cleveland Heights, OH 44121

For the applicant,

Gerald E. Linden 5/5/05
Gerald E. Linden, Reg 30,282 date
(561) 694-2094

10990296

PLUS Search Results for S/N 10990296, Searched July 05, 2005

The Patent Linguistics Utility System (PLUS) is a USPTO automated search system for U.S. Patents from 1971 to the present. PLUS is a query-by-example search system which produces a list of patents that are most closely related linguistically to the application searched. This search was prepared by the staff of the Scientific and Technical Information Center, SIRA.

6439464
6128673
6343364
6883715
6131125
6370603
6567273
6628325
6694399
6750902
6752321
6769622
6772956
6843423
6910638
6098171
6151647
6168077
6199128
6581122
6634565
6738259
6763399
6779059
6801956
6817534
6883718
6598032
6748541
6779734
6874680
6543690
6783078
6793144
6913196
6914695
6205505
5875313
5937175
5953511
5968142
6058441
6125409
6286063
6385677
6625472
6629181
6658516
6731751
6738856

6745267
6061746
6061746
5841471
5890016
5930496
5933656
5951667
5963726
5970220
5987106
6073188
6085156
6105143
6178458
6192420
6199122
6206480
6217389
6223134
6217389
6223134
6243778
6246578
6251014
6270415
6289405
6292863
6301104
6343260
6356968
6405145
6418392
6424525
6443839
6449662
6480801
6524137
6525932
6546441
6557754
6581123
6607139
6614708
6651184
6654841
6676420
6712698
6722985
6736678

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/990,296	11/16/2004	Dennis J. Ryan	Ryan C-4	2050

37053 7590 07/12/2005

D.A. STAUFFER PATENT SERVICES LLC
1006 MONTFORD ROAD
CLEVLAND HTS., OH 44121-2016

EXAMINER	
LE, UYEN CHAU N	
ART UNIT	**PAPER NUMBER**
2876	

DATE MAILED: 07/12/2005

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

PTO-90C (Rev. 10/03)

AK

Office Action Summary	Application No.	Applicant(s)	
	10/990,296	RYAN ET AL.	
	Examiner	Art Unit	
	Uyen-Chau N. Le	2876	

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)□ Responsive to communication(s) filed on _____.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1-52 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1-52 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____.
5) □ Notice of Informal Patent Application (PTO-152)
6) □ Other: _____.

DETAILED ACTION

Claim Objections

1. Claims 2, 3, 11, 12, 15, 16, 23, 24, 27-31, 33, 35-38, 40 and 43-46 are objected to because of the following informalities:

Re claim 2, line 2: Delete "a".

Re claim 3, line 2: Delete "a".

Re claim 11, line 2: Substitutes "to that the device" with -- so that the personal token apparatus --.

Re claim 12, line 2: Substitutes "the modules" with -- the connection, translation, processor and input/output modules --.

Re claim 12, line 2: Substitutes "the form" with -- a form --.

Re claim 12, line 2: Substitutes "the general" with -- a general --.

Re claim 15, line 2: Substitutes "capable of" with -- configured for --.

Re claim 16, line 5: Substitutes "the apparatus" with -- the personal token apparatus --.

Re claim 23, line 3: Substitutes "the command" with -- a command --.

Re claim 23, line 10: Substitutes "its" with -- a --.

Re claim 24, line 2: Substitutes "the contactless/wireless module" with -- the contactless/wireless interface --.

Re claim 24, line 2: Substitutes "Interface" with -- interface --.

Re claim 27, line 2: Delete "of".

Re claim 28, line 3: Substitutes “the command” with -- a command --.

Re claim 29, line 2: Substitutes “the contactless/wireless module” with -- the contactless/wireless interface --.

Re claim 29, line 2: Substitutes “Interface” with -- interface --.

Re claim 30, line 7: Substitutes “the personal token” with -- the personal token apparatus --.

Re claim 30, line 8: Substitutes “the personal token” with -- the personal token apparatus --.

Re claim 31, line 2: Substitutes “the personal token” with -- the personal token apparatus --.

Re claim 33, line 3: Delete “(for example, event tickets)”.

Re claim 35, line 2: Substitutes “the personal token” with -- the personal token apparatus --.

Re claim 36, line 3: Substitutes “the personal token” with -- the personal token apparatus --.

Re claim 37, line 2: Substitutes “the personal token” with -- the personal token apparatus --.

Re claim 38, line 3: Substitutes “the personal token” with -- the personal token apparatus --.

Re claim 40, line 3: Substitutes “the command” with -- a command --.

Re claim 43, line 2: Substitutes “such as” with -- including --.

Re claim 44, line 3: Substitutes “the command” with -- a command --.

Re claim 45, line 2: Substitutes "(e.g., contact, contactless, USB) processor" with -- processor including contact, contactless, USB) --.

Re claim 46, line 3: Delete "a".

Appropriate correction is required.

Claim Rejections - 35 USC § 112

2. Claim 32 is rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Re claim 32, line 2: "the downloaded information" lacks antecedent basis because none of the previous claims, which the claim depends on, recites any downloading information.

Claim Rejections - 35 USC § 102

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

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

4. Claims 1-7, 9, 12-16, 21, 41-44 and 46-51 are rejected under 35 U.S.C. 102(e) as being anticipated by Margalit et al (US 6,748,541).

Re claims 1-7, 9, 12-16, 21, 41-44 and 46-51: Margalit et al discloses a compact personal token apparatus 125, comprising; a connection module 140; a translation module, which incorporated with a processor module 130; and an input/output module (fig. 2); wherein: the connection module 140 is for interfacing the personal token apparatus with a an Internet-capable appliance; and the interface is a USB interface (fig. 2); wherein: the connection module 140 is for interfacing the personal token apparatus with a an Internet-capable appliance; and the Internet-capable appliance comprises a device, which is a personal computer (PC); wherein: the translation module moves signals between a USB interface and a smart card interface (fig. 2; col. 5, lines 1-30); wherein: the smart card interface 170 is an ISO 7816; wherein: the processor module 130 comprises a dual interface (DI) chip (i.e., USB and smart card); wherein: the processor module 130 incorporates the translation module (i.e., for passing data from the smart card to the USB interface chip 140 and vice versa) (fig. 2; col. 5, lines 20-27); flash memory 150 (fig. 2; col. 4, lines 35-38); a first physical module containing the input module and the translation module; and a second physical module containing the processor module and the output module (fig. 3); wherein: the connection, translation, processor, and input/output modules are embodied in a form of an apparatus having a general physical configuration of a conventional USB memory fob (figs. 3-5B); wherein: the output module comprises contacts for interfacing with a smart card (fig. 2); the fob is configured for interfacing with the Internet and emulating a smart card (fig. 2); wherein: the connection module 140 is for interfacing the personal token apparatus with an Internet-capable appliance; and further comprising: an input module is for connecting to the Internet; and the apparatus incorporates firewall functionality to protect the Internet-capable appliance (i.e., login process including username and password) (fig. 5B); a standard-compliant contact based interface, the contact based interface complying to at least one standard interface selected from the group consisting of USB, IEEE 1394, PCMCIA, Compact Flash, Multi Media, Memory Stick, Smart Media, Secure Digital, mini SD, IBM Micro Drive, and any similar standard interface (fig. 2).

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

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

6. Claims 1, 8, 10, 11, 18-29 and 31-40 are rejected under 35 U.S.C. 102(e) as being anticipated by Jiau (US 2003/0236821 A1).

Re claims 1, 8, 10, 11, 18-29 and 31-40: Jiau discloses a compact personal token apparatus 1, comprising: a connection module 1312 (paragraph [0044]); a translation module, which incorporated with a processor module 132; and an input/output module [139, 1341, 1342, 1343, 1344] (figs. 1 & 3A-3C); the translation module moves signals between a USB interface and a wireless interface (paragraphs [0050-0051]); an LCD screen 1341 and LEDs 1342 (fig. 3C); a standard-compliant contact based interface, the contact based interface complying to at least one standard interface selected from the group consisting of USB, IEEE 1394, PCMCIA, Compact Flash, Multi Media, Memory Stick, Smart Media, Secure Digital, mini SD, IBM Micro Drive, and any similar standard interface (paragraph [0044]); a standard-compliant contactless/wireless interface 1311; the contactless/wireless interface 1311 complying to one or more of the following standard interfaces: RFID-contactless interface according to WLAN 812.11 and Bluetooth compatible interface (paragraphs [0047] & [0050]); a flash memory 133 (fig. 3A); wherein: the dual interface chip (processor) inside the personal token can be directly programmed by a software running on the host system using the interface processor without the need for an external contact based dual interface read/write device (paragraph [0052]); wherein: the downloaded information can be used in the real world; wherein: the software is web based, allowing for downloading information from the web directly into the dual interface processor memory thus linking the virtual world to the real world (paragraph [0052]); wherein: the information stored in the personal token via the standard contact based interface is used for personal identification, secure network logon, access control, e-ticketing, e-payment and similar applications using either the standard compliant interface or the RFID-compliant interface (paragraph [0067]).

Claim Rejections - 35 USC § 103

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

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

8. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

9. Claims 17, 45 and 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Margalit et al in view of Jiau. The teachings of Margalit et al and Jiau have been discussed above.

Re claims 17, 45 and 52: Margalit et al has been discussed above but is silent with respect to a contactless interface.

Jiau teaches a communication unit 131 includes wireless connection 1311 (fig. 3B; paragraph [0051]).

It would have been obvious to an artisan of ordinary skill in the art at the time the invention was made to incorporate a wireless connection of Jiau into the system as taught by Margalit et al in order to provide Margalit et al with a universal system wherein the system can be utilized in any type of communications (i.e., contact, contactless, USB, etc.). Furthermore, such modification would provide the user the flexibility in using the system wherein the user does not have to concern about whether or not the system is compatible with a particular communication system that the user intend to use, and therefore an obvious expedient.

10. Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jiau in view of Margalit et al. The teachings of Jiau and Margalit et al have been discussed above.

Re claim 30: Jiau has been discussed above but is silent with respect to an interface that is complying to ISO 7810 or a 7816 compliant SIM module.

Margalit et al teaches a personal token apparatus 125 having an interface that is a 7816 compliant SIM module (fig. 2).

It would have been obvious to an artisan of ordinary skill in the art at the time the invention was made to incorporate a 7816 compliant SIM module of Margalit et al into the system as taught by Jiau in order to provide Jiau with a universal system wherein the system can be utilized in any type of communications (i.e., contact, contactless, USB, etc.). Furthermore, such modification would provide the user the flexibility in using the system wherein the user does not have to concern about whether or not the system is compatible with a particular communication system that the user intend to use, and therefore an obvious expedient.

Conclusion

11. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

The patents to Elteto et al (US 20010043702 A1); Hoornaert et al (US 20010054148 A1); Sazawa et al (JP 2004246720 A); Long et al (US 6848045 B2); Abbott et al (WO 200196990 A); Gray et al (US 6168077 B1); Silverman et al (US 6370603 B1); Yao (US 6385677 B1); Leydier et al (US 6543690 B2); Liu et al (US 6567273 B1); Yao (US 6658516 B2); Leydier et al (US 6694399 B1); Leaming (US 6752321 B1); Margalit et al (US 6763399 B2); Leaming (US 6772956 B1); Feuser et al (US 6801956 B2); Liu et al (US 6676420 B1); Tordera et al (US 6879597 B2) are cited as of interest and illustrate a similar structure to a multi-interface compact personal token apparatus and methods of use.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Uyen-Chau N. Le whose telephone number is 571-272-2397. The examiner can normally be reached on Mon-Fri. 5:30AM-2:00PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael G. Lee can be reached on 571-272-2398. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Uyen-Chau N. Le
Examiner
Art Unit 2876

July 7, 2005

Notice of References Cited	Application/Control No. 10/990,296	Applicant(s)/Patent Under Reexamination RYAN ET AL.	
	Examiner Uyen-Chau N. Le	Art Unit 2876	Page 1 of 2

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-2001/0043702 A1	11-2001	Elteto et al.	380/278
	B	US-2001/0054148 A1	12-2001	Hoornaert et al.	713/172
	C	US-6,748,541 B1	06-2004	Margalit et al.	713/201
	D	US-6,848,045 B2	01-2005	Long et al.	713/200
	E	US-6,168,077 B1	01-2001	Gray et al.	235/375
	F	US-6,370,603 B1	04-2002	Silverman et al.	710/72
	G	US-6,385,677 B1	05-2002	Yao, Li-Ho	711/115
	H	US-6,543,690 B2	04-2003	Leydier et al.	235/451
	I	US-6,567,273 B1	05-2003	Liu et al.	361/737
	J	US-6,658,516 B2	12-2003	Yao, Li-Ho	710/301
	K	US-6,694,399 B1	02-2004	Leydier et al.	235/492
	L	US-6,752,321 B1	06-2004	Leaming, Taylor J.	235/492
	M	US-6,763,399 B2	07-2004	Margalit et al.	710/13

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
✓	N	JP 2004246720 A	09-2004	Japan	SAZAWA et al.	G06F 09/445
✓	O	WO 200196990 A2	12-2001	World Intellect	ABBOTT et al.	G06F 01/00
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

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

Notice of References Cited	Application/Control No. 10/990,296	Applicant(s)/Patent Under Reexamination RYAN ET AL.	
	Examiner Uyen-Chau N. Le	Art Unit 2876	Page 2 of 2

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-6,772,956 B1	08-2004	Leaming, Taylor J.	235/492
	B	US-6,801,956 B2	10-2004	Feuser et al.	235/492
	C	US-6,676,420 B1	01-2004	Liu et al.	439/131
	D	US-2003/0236821 A1	12-2003	Jiau, Goun-Zong	709/203
	E	US-6,879,597 B2	04-2005	Tordera et al.	370/463
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

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

PAT-NO: JP02004246720A

DOCUMENT-IDENTIFIER: JP 2004246720 A

TITLE: INFORMATION PROCESSING DEVICE, INFORMATION PROCESSING METHOD AND PROGRAM

PUBN-DATE: September 2, 2004

INVENTOR-INFORMATION:

NAME	COUNTRY
SAZAWA, SHINICHI	N/A
SATO, YUICHI	N/A
SENDA, YOSUKE	N/A

INT-CL (IPC): G06F009/445, G06F001/00 , G06F013/10 , G06F015/00

ABSTRACT:

PROBLEM TO BE SOLVED: To easily construct, in an arbitrary personal computer, a personal working environment of groupware or the like requiring personal identification, and make it usable.

SOLUTION: An information processing device referred to as a peer token 10 has a port connector which can be freely detached from/attached to a device port of a personal computer 12 which can perform power supply and data transfer; a first radio communication part which sends/receives information via a wireless circuit to/from an external device; a second radio communication part which sends/receives information to/from the external device using a wireless circuit different from that for the first radio communication part; and a non-volatile memory 34 storing a device driver 44, a USB driver 54, an personal identification library 48, groupware 46, a first radio communication driver and a second radio communication driver. When the peer token 10 is connected to the device port of the personal computer 12, an application program is installed in the personal computer 12 via the personal identification by the installation of the device driver and then the personal identification library, and is then executed by the computer.

(19)日本国特許庁(JP)　(12)公 開 特 許 公 報(A)　(11)特許出願公開番号
特開2004-246720
(P2004-246720A)
(43)公開日　平成16年9月2日(2004.9.2)

(51) Int.Cl.⁷	F I			テーマコード（参考）
G06F 9/445	G06F	9/06	610A	5B014
G06F 1/00	G06F	13/10	330B	5B076
G06F 13/10	G06F	15/00	330B	5B085
G06F 15/00	G06F	15/00	390	
	G06F	9/06	610L	

審査請求 未請求　請求項の数 5　ＯＬ　（全 23 頁）　最終頁に続く

(21) 出願番号　特願2003-37225 (P2003-37225)
(22) 出願日　平成15年2月14日 (2003.2.14)

(71) 出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番
１号
(74) 代理人　100079359
弁理士　竹内　進
(72) 発明者　佐沢　真一
神奈川県川崎市中原区上小田中４丁目１番
１号　富士通株式会社内
(72) 発明者　佐藤　裕一
神奈川県川崎市中原区上小田中４丁目１番
１号　富士通株式会社内
(72) 発明者　千田　陽介
神奈川県川崎市中原区上小田中４丁目１番
１号　富士通株式会社内

最終頁に続く

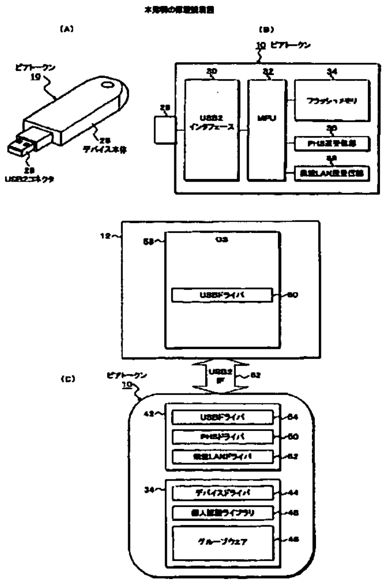
(54)【発明の名称】情報処理デバイス、情報処理方法及びプログラム

(57)【要約】

【課題】任意のパーソナルコンピュータに個人認証を必要とするグループウェア等の個人の作業環境を簡単に構築して利用可能とする。

【解決手段】ピアトークン１０と呼ばれる情報処理デバイスは、電源供給とデータ転送が可能なパーソナルコンピュータ１２のデバイスポートに対し着脱自在なポートコネクタと、外部装置に対し無線回線により情報を送受する第１無線通信部と、外部装置に対し第１無線通信部とは異なる無線回線を使用して情報を送受する第２無線通信部と、デバイスドライバ４４、ＵＳＢドライバ５４、個人認証ライブラリ４８、グループウェア４６、第１無線通信用ドライバ及び第２無線通信用ドライバを格納した不揮発メモリ３４をもつ。ピアトークン１０をパーソナルコンピュータ１２のデバイスポートに接続すると、デバイスドライバのインストール、個人認証ライブラリのインストールによる個人認証を経てアプリケーションプログラムをインストールして実行させる。

【選択図】　　図１



【特許請求の範囲】

【請求項１】

電源供給とデータ転送が可能な情報処理装置のデバイスポートに対し着脱自在なポートコネクタと、

外部装置に対し無線回線により情報を送受する第１無線通信部と、

外部装置に対し前記第１無線通信部とは異なる無線回線を使用して情報を送受する第２無線通信部と、

デバイスドライバ、ポートドライバ、個人認証ライブラリ、任意のアプリケーションプログラム、第１無線通信用ドライバ及び第２無線通信用ドライバを格納した不揮発メモリと、

前記ポートコネクタを情報処理装置のデバイスポートに接続した際に起動し、前記情報端末装置からの最初のデバイスアクセスに対し前記デバイスドライバを転送してインストールさせ、インストールされた前記デバイスドライバにより前記個人認証ライブラリをインストールさせて個人認証を行わせ、個人認証に成功した場合に前記アプリケーションプログラムをインストールして実行させ、前記認証ライブラリ及びアプリケーションプログラムの実行による外部装置とのアクセスを前記第１又は第２無線通信用ドライバにより行わせ、アプリケーションの終了時には前記デバイスドライバ、個人認証ライブラリ及びアプリケーションプログラムをアンインストールさせるデバイス処理部と、

を備えたことを特徴とする情報処理デバイス。

【請求項２】

請求項１記載の情報処理デバイスに於いて、前記アプリケーションプログラムは複数の情報処理装置でデータを共有するピアツーピア型のグループウェア処理プログラムであることを特徴とする情報処理デバイス。

【請求項３】

請求項１記載の情報処理デバイスに於いて、前記不揮発メモリに自己の情報処理装置で使用しているファイルをサーバに格納したことを示すディレクトリ情報を登録し、前記アプリケーションプログラムは、他の情報処理装置の差込み時に、前記レジストリ情報により前記サーバからファイルを取得して前記自己の情報処理装置の作業環境を構築することを特徴とする情報処理デバイス。

【請求項４】

電源供給とデータ転送が可能な情報処理装置のデバイスポートに対し着脱自在なポートコネクタと、外部装置に対し無線回線により情報を送受する第１無線通信部と、外部装置に対し前記第１無線通信部とは異なる無線回線を使用して情報を送受する第２無線通信部と、デバイスドライバ、ポートドライバ、個人認証ライブラリ、任意のアプリケーションプログラム、第１無線通信用ドライバ及び第２無線通信用ドライバを格納した不揮発メモリとを備えた情報処理デバイスの情報処理方法に於いて、

前記ポートコネクタを情報処理装置のデバイスポートに接続した際に起動し、前記情報端末装置からの最初のデバイスアクセスに対し前記デバイスドライバを転送してインストールさせる起動ステップと、

インストールされた前記デバイスドライバにより前記個人認証ライブラリをインストールさせて個人認証を行わせる個人認証ステップと、

個人認証に成功した場合に前記アプリケーションプログラムをインストールして実行させる実行ステップと、

前記認証ライブラリ及びアプリケーションプログラムの実行による外部装置とのアクセスを前記第１又は第２無線通信用ドライバにより行わせる通信ステップと、

アプリケーションプログラムの終了時に前記デバイスドライバ、個人認証ライブラリ及びアプリケーションプログラムをアンインストールさせるアンインストールステップと、

を備えたことを特徴とする情報処理方法。

【請求項５】

電源供給とデータ転送が可能な情報処理装置のデバイスポートに対し着脱自在なポートコ

ネクタと、外部装置に対し無線回線により情報を送受する第１無線通信部と、外部装置に対し前記第１無線通信部とは異なる無線回線を使用して情報を送受する第２無線通信部と、デバイスドライバ、ポートドライバ、個人認証ライブラリ、任意のアプリケーションプログラム、第１無線通信用ドライバ及び第２無線通信用ドライバを格納した不揮発メモリとを備えた情報処理デバイスのコンピュータに、

前記ポートコネクタを情報処理装置のデバイスポートに接続した際に起動し、前記情報端末装置からの最初のデバイスアクセスに対し前記デバイスドライバを転送してインストールさせる起動ステップと、

インストールされた前記デバイスドライバにより前記個人認証ライブラリをインストールさせて個人認証を行わせる認証ステップと、

個人認証に成功した場合に前記アプリケーションプログラムをインストールして実行させる実行ステップと、

前記認証ライブラリ及びアプリケーションプログラムの実行による外部装置とのアクセスを前記第１又は第２無線通信用ドライバにより行わせる通信ステップと、

アプリケーションプログラムの終了時に前記デバイスドライバ、個人認証ライブラリ及びアプリケーションプログラムをアンインストールさせるアンインストールステップと、

を実行させることを特徴とするプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、任意のパーソナルコンピュータに対し個人のコンピュータ環境を構築する携帯型の情報処理デバイス、情報処理方法及びプログラムに関し、特に、ピアツーピア型のグループウェアのコンピュータ環境を簡単に構築する情報処理デバイス、情報処理方法及びプログラムに関する。

【０００２】

【従来の技術】

従来、自分のパーソナルコンピュータと同じ環境を出張などの外出先で実現する方法としては、ラップトップやＰＤＡといった携帯型のデバイスに個別に自己の作業環境を構築しておき、事前に作業に必要なデータを日常的に使用しているデスクトップ等からメールの添付や無線回線などを利用して転送し、これを持ち運んで使用している。

【０００３】

また出張先によっては、そこに設置しているデスクトップ等を自由に使用できる場合があることから、文書入力といった汎用的なアプリケーションで足りる場合には、パーソナルコンピュータを借用して作業することができる。

【０００４】

【特許文献１】

販売元株式会社サクセス、製造元エニワン株式会社、“ＵＳＢストレージ［ビー・エニィウェアー］”、［平成１５年２月３日検索］、インターネット＜ＵＲＬ：ＨＹＰＥＲＬＩＮＫ ｈｔｔｐ：／／ｂｅｅｍａｉｌ．ｊｐ／ａｎｙｗｈｅｒｅ．ｈｔｍｌ ＵＲＬ：／／ｗｗｗ．ｂｅｅｍａｌ．ｊｐ／／ａｎｙｗｈｅｒｅ．ｈｔｍｌ＞

【０００５】

【発明が解決しようとする課題】

しかしながら、パーソナルコンピュータの環境は、デスクトップやラップトップといったパーソナルコンピュータ毎に固有な場合がほとんどであり、例えば、メールの場合、事務所等に設置して使用しているデスクトップと出張に持ち歩くラップトップとでは、アドレス帳などの環境や受信メール本体に常に差分が生じてしまい、非常に不便な状況が発生している。

【０００６】

このような問題を解決するため、例えばウェブメールやＩＭＡＰ４等のプロトコルによるサーバによる一元管理の方法もあるが、一元管理に伴う個人毎の容量制限やクライアント

・サーバモデルによる反応速度の低下といった問題がある。

【０００７】

また持ち歩いているラップトップにつき、無線ＬＡＮやＰＨＳを使ってメール等を通信する場合、それぞれ専用のパーソナルコンピュータ向けのＭＣＩＡカードが必要であり、場合によってはパーソナルコンピュータ毎にドライバソフトのインストールし、必要な設定作業を行うといった面倒な作業が要求される。

【０００８】

更に、サーバ等にアクセスしてデータを利用する場合、通常、ＩＤとパスワードを入力する個人認証を必要とし、そのため出張時にラップトップを使用する場合にも煩雑な認証操作が必要となる。この問題を解消するものとしてＵＳＢトークンまたはＩＣカードによる個人認証デバイスが存在する。しかし、これらの個人認証デバイスは、個人認証を行う機能に限られており、個人のコンピュータ環境の構築には対応していない。

【０００９】

一方、メモリステックのようにメモリのみを内蔵したカードやトークンも存在するが、これらは単なるメモリ機能しか持たず、個人のコンピュータ環境の構築には対応していない。

【００１０】

更にＵＳＢの内部にメールソフトを予めインストールしたデバイスも存在するが（特許文献１）、用途がメールに限られており、認証を含む汎用的なアプリケーションに対応したコンピュータ環境の構築には対応できない。

【００１１】

本発明は、任意のパーソナルコンピュータに個人認証を必要とするグループウェア等の個人の作業環境を簡単に構築して利用できる情報処理デバイス、情報処理方法及びプログラムを提供することを目的とする。

【００１２】

【課題を解決するための手段】

図１（Ａ）（Ｂ）（Ｃ）は本発明の原理説明図である。本発明の情報処理デバイス（ピアトークン１０）は、電源供給とデータ転送が可能な情報処理装置のデバイスポートに対し着脱自在なポートコネクタと、外部装置に対し無線回線により情報を送受する第１無線通信部（ＰＨＳ送受信部３６）と、外部装置に対し第１無線通信部とは異なる無線回線を使用して情報を送受する第２無線通信部（無線ＬＡＮ送受信部３８）と、デバイスドライバ４４、ポートドライバ、個人認証ライブラリ４８、任意のアプリケーションプログラム、第１無線通信用ドライバ及び第２無線通信用ドライバを格納した不揮発メモリ（フラッシュメモリ３４）と、ポートコネクタを情報処理装置（パーソナルコンピュータ１２）のデバイスポートに接続した際に起動し、情報端末装置からの最初のデバイスアクセスに対しデバイスドライバを転送してインストールさせ、インストールされたデバイスドライバにより個人認証ライブラリをインストールさせて個人認証を行わせ、個人認証に成功した場合にアプリケーションプログラムをインストールして実行させ、認証ライブラリ及びアプリケーションプログラムの実行による外部装置とのアクセスを第１又は第２無線通信用ドライバにより行わせ、アプリケーションの終了時には前記デバイスドライバ、個人認証ライブラリ及びアプリケーションプログラムをアンインストールさせるデバイス処理部とを備えたことを特徴とする。

【００１３】

このため本発明は、情報処理デバイスを任意のパーソナルコンピュータやＰＤＡ等のデバイスポートに差し込むだけで、個人認証画面が自動的に立ち上がり、個人認証を済ませた後は、グループウェア等のアプリケーション画面が立ち上がり、外部との送受信を含む作業をすぐ始めることができる。

【００１４】

また無線通信機能が二重化されており、使用場所の無線環境に合わせて自動切換えして外部装置に確実にアクセスできる。

【００１５】
更にアプリケーションの実行で使用されたデータは全て不揮発メモリに保存され、また本発明のデバイスを抜いて処理を終えると、パーソナルコンピュータにインストールしたプログラムやドライバは全てアンインストールされ、本発明のデバイスを差し込んで使用したパーソナルコンピュータ本体の環境をまったく侵蝕することがない。

【００１６】
ここでデバイス本体２６は持ち運び自在なキー型である。またデバイスポートは例えばＵＳＢ２コネクタ２８であり、ポートドライバはＵＳＢドライバ５４である。更に第１無線通信部はＰＨＳ無線回線を使用するＰＨＳ送受信部３６であり、第２無線通信部は無線ＬＡＮを使用する無線ＬＡＮ送受信部３８である。

【００１７】
本発明の情報処理デバイスによりインストールするアプリケーションプログラムは、複数の情報処理装置でデータを共有するピアツーピア型のグループウェア４６の処理プログラムである。

【００１８】
このようにアプリケーションプログラムがグループウェア処理プログラムの場合、個人認証ライブラリは第１又は第２無線通信部により外部の認証サーバに接続して認証処理を実行させる。

【００１９】
グループウェア処理プログラムは、不揮発メモリに共有データを保持し、起動時にグループウェアに属している他の情報処理装置の保持している共有データとの同期をとる。即ち、グループウェア処理プログラムは、自己の共有データと他の情報処理装置との非同期を検知した場合、他の装置から差分データを受信してマージすることにより共有データの同期をとる。このため出張先のコンピュータを使用する際にも、最新の共有データを利用できる。

【００２０】
グループウェア処理プログラムは、使用済みファイルを不揮発メモリに格納する際にメモリ容量の不足を検知した場合、ファイルリストの末尾に格納しているファイルをグループウェアに属する他の情報処理装置に転送した後にファイルを消去して保存先のリンク情報を格納し、その後に使用済みファイルをファイルリストの先頭位置に格納する。

【００２１】
このためデバイス内蔵メモリに制約があっても、グループウェアに属する例えば近隣のピア装置となるパーソナルコンピュータに共有データを転送保持させ、そのリンク情報のみをデバイス内に保持することで、メモリ容量に制限があっても共有データを確実に保存できる。このデバイスの不揮発性メモリに保持したリンク情報は、自分のパーソナルコンピュータを使用する際に、本発明のデバイスを差し込むことによりリンク情報で指定される保存先から実データを取得して保持することができる。

【００２２】
また情報処理デバイスにあっては、不揮発メモリに自己の情報処理装置で使用しているファイルをサーバに格納したことを示すレジストリ情報を登録し、アプリケーションプログラムは、他の情報処理装置の差込み時に、不揮発メモリに登録しているレジストリ情報によりサーバからファイルを取得して自己の処理装置の作業環境を構築する。

【００２３】
本発明の別の形態にあっては、情報処理デバイスのポートコネクタにより接続する情報処理装置は携帯電話であり、この場合、アプリケーションプログラムは、交通機関の改札ゲートの通過時にゲート開制御と課金処理を行うことを特徴とする。また情報処理デバイスのポートコネクタにより接続する情報処理装置は携帯電話であり、アプリケーションプログラムは、自動販売機との間で商品の購入処理を行うことを特徴とする。このように交通機関の改札や自動販売機の利用につき、無線機能を利用した処理が簡単にできる。

【００２４】

本発明は任意のパーソナルコンピュータにグループウェア等の個人の作業環境を簡単に構築して利用できる情報処理方法を提供する。

【0025】

即ち、本発明は、電源供給とデータ転送が可能な情報処理装置のデバイスポートに対し着脱自在なポートコネクタと、外部装置に対し無線回線により情報を送受する第１無線通信部と、外部装置に対し第１無線通信部とは異なる無線回線を使用して情報を送受する第２無線通信部と、デバイスドライバ、ポートドライバ、個人認証ライブラリ、任意のアプリケーションプログラム、第１無線通信用ドライバ及び第２無線通信用ドライバを格納した不揮発メモリとを備えたデバイスの情報処理方法であって、

ポートコネクタを情報処理装置のデバイスポートに接続した際に起動し、情報端末装置からの最初のデバイスアクセスに対しデバイスドライバを転送してインストールさせる起動ステップと、

インストールされたデバイスドライバにより個人認証ライブラリをインストールさせて個人認証を行わせる認証ステップと、

個人認証に成功した場合にアプリケーションプログラムをインストールして実行させる実行ステップと、

認証ライブラリ及びアプリケーションプログラムの実行による外部装置とのアクセスを第１又は第２無線通信用ドライバにより行わせる通信ステップと、

アプリケーションプログラムの終了時にデバイスドライバ、個人認証ライブラリ及びアプリケーションプログラムをアンインストールさせるアンインストールステップと、

を備えたことを特徴とする。

【0026】

本発明は、任意のパーソナルコンピュータにグループウェア等の個人の作業環境を簡単に構築して利用できるコンピュータで実行されるプログラムを提供する。

【0027】

即ち、本発明のプログラムは、電源供給とデータ転送が可能な情報処理装置のデバイスポートに対し着脱自在なポートコネクタと、外部装置に対し無線回線により情報を送受する第１無線通信部と、外部装置に対し第１無線通信部とは異なる無線回線を使用して情報を送受する第２無線通信部と、デバイスドライバ、ポートドライバ、個人認証ライブラリ、任意のアプリケーションプログラム、第１無線通信用ドライバ及び第２無線通信用ドライバを格納した不揮発メモリとを備えた情報処理デバイスのコンピュータに、

ポートコネクタを情報処理装置のデバイスポートに接続した際に起動し、情報端末装置からの最初のデバイスアクセスに対しデバイスドライバを転送してインストールさせる起動ステップと、

インストールされた前記デバイスドライバにより個人認証ライブラリをインストールさせて個人認証を行わせる認証ステップと、

個人認証に成功した場合にアプリケーションプログラムをインストールして実行させる実行ステップと、

認証ライブラリ及びアプリケーションプログラムの実行による外部装置とのアクセスを第１又は第２無線通信用ドライバにより行わせる通信ステップと、

アプリケーションプログラムの終了時にデバイスドライバ、個人認証ライブラリ及びアプリケーションプログラムをアンインストールさせるアンインストールステップと、

を実行させることを特徴とする。

【0028】

なお、本発明の情報処理方法及びプログラムの詳細は、情報処理デバイスと基本的に同じになる。

【0029】

【発明の実施の形態】

図２は、本発明によるピアトークンと呼ばれる情報処理デバイスが適用されるシステム環境の説明図である。

【００３０】
図２において、本発明の処理デバイスはピアトークン１０として実現されている。ピアトークン１０は無線ＬＡＮとＰＨＳの二重化された通信機能を持ち、個人認証環境及びグループウェアシステム環境を不揮発メモリ上に内蔵したトークン型の外部ペリフラル装置である。

【００３１】
このピアトークン１０は、例えば出張先で使用することのできるパーソナルコンピュータで１２のＵＳＢ２ポートに差し込むことで、使用先となるパーソナルコンピュータ１２の環境を犯すことなく認証作業を行い、且つグループウェアシステム環境をパーソナルコンピュータ１２上に構築し、ピアツーピア型のグループウェアによる処理を可能とする。

【００３２】
このようなピアトークン１０の使用環境にあっては、ピアトークン１０の無線ＬＡＮ及びＰＨＳの通信機能を利用して、ＰＨＳ基地局２０または無線ＬＡＮに対応したホットスポット２２との間に通信回線を確立し、インターネット１６を経由して例えばプロキシサーバ１８を介したＬＡＮ１５に接続されているグループウェアに属するピア装置１４－１～１４－３や、インターネット１６に直接接続されるピア装置１４－４との間でデータを共有するグループウェアシステムを構築する。また、ピアトークン１０を使用先となるパーソナルコンピュータ１２に差し込んだ際の個人認証の処理に対応し、インターネット１６を介して認証サーバ２４が設けられている。

【００３３】
図３は、本発明によるキー型のピアトークン１０の外観を示している。ピアトークン１０は、樹脂成型されたパッケージによるデバイス本体２６をキー型に構成し、デバイス本体２６の一端にパーソナルコンピュータやＰＤＡなどの情報処理装置に接続するためのデバイスコネクタとして例えばＵＳＢ２コネクタ２８を設けている。

【００３４】
ここでＵＳＢ２インタフェースは、パーソナルコンピュータ及びＰＤＡ側のＵＳＢ２ポートに対するコネクタ接続でピアトークン１０に対し電源供給を行うと同時にデータ転送を行うことができる。

【００３５】
図４は、本発明によるピアトークン１０のハードウェア構成のブロック図である。図４において、ピアトークン１０にはパーソナルコンピュータやＰＤＡに差し込むためのＵＳＢ２コネクタ２８が設けられ、これに続いてＵＳＢ２インタフェース３０及びＭＰＵ３２が設けられている。

【００３６】
ＭＰＵ３２に対しては、不揮発メモリであるフラッシュメモリ３４が接続される。またＭＰＵ３２に対しては、外部装置との無線回線によるデータ転送を行うためＰＨＳ送受信部３６と無線ＬＡＮ送受信部３８が設けられている。

【００３７】
図５は、図４のフラッシュメモリ３４の格納内容となるメモリマップの説明図である。このメモリマップ４０に示すように、フラッシュメモリ３４には、デバイス処理プログラム４２、デバイスドライバ４４、アプリケーションプログラムとしてのグループウェア４６、個人認証ライブラリ４８、ＰＨＳドライバ５０、無線ＬＡＮドライバ５２及びＵＳＢドライバ５４が予め格納されている。

【００３８】
このようなプログラム領域に続く残りの領域はデータ領域５５となっており、この実施形態のアプリケーションであるグループウェアシステム環境の構築により送受信されたファイルデータが格納される。このデータ領域は、グループウェアシステム環境の場合には、右側に取り出して示すようにファイルリスト５６と実データ域５７で構成されている。

【００３９】
ここで、メモリマップ４０の先頭に格納されているデバイス処理プログラム４２は、ＭＰ

Ｕ３２による実行でピアトークン１０のＯＳとなるデバイス処理部として動作する。次のデバイスドライバ４４は、ピアトークン１０をパーソナルコンピュータやＰＤＡに差し込んだ際のピアトークン１０とのやり取りを行うためのプログラムであり、パーソナルコンピュータやＰＤＡ側にこのデバイスドライバ４４がない場合には、初期処理によりデバイスドライバ４４をインストールして、ピアトークン１０とのやり取りを行わせる。

【００４０】

グループウェア４６はアプリケーションプログラムであり、パーソナルコンピュータやＰＤＡ側にインストールされたデバイスドライバ４４の処理により差し込み先にダウンロードされてグループウェアシステム環境を作り、ピアツーピア型のデータ共有による送受信を行う。

【００４１】

個人認証ライブラリ４８は、グループウェア４６のインストールに先立つ個人認証処理のために差込み先にインストールされ、認証画面を開くことでユーザによるＩＤとパスワードの入力を受け、外部の認証サーバ２４とのやり取りで認証処理を行う。

【００４２】

ＰＨＳドライバ５０は図４のＰＨＳ送受信部３６を動作し、図２のようにＰＨＳ基地局２０との間に無線回線を確立して、ピアトークン１０の差込みで個人認証ライブラリ４８及びグループウェア４６がインストールされた使用先となるパーソナルコンピュータ１２のグループウェアシステム環境における例えば認証サーバ２４との間の認証のための通信、あるいはピア装置１４－１～１４－４との間のピアツーピアのデータ送受信を行う。

【００４３】

無線ＬＡＮドライバ５２は、図４の無線ＬＡＮ送受信部３８を制御し、図２のホットスポット２２との間で無線回線を確立し、同じくグループウェアシステム環境における個人認証処理や他のピア装置１４－１～１４－４との間のデータ共有のための送受信を行う。

【００４４】

このＰＨＳドライバ５０と無線ＬＡＮドライバ５２は、２つの無線回線を切り替えて使用するために設けられており、ピアトークン１０を差し込んだパーソナルコンピュータやＰＤＡの使用環境に応じ、いずれか一方の通信回線を自動的に選択して外部装置との間の送受信を行う。

【００４５】

図６は、本発明のピアトークン１０をパーソナルコンピュータ１２に差し込んでＵＳＢ２インタフェース６２による接続を確立した起動時の説明図である。パーソナルコンピュータ１２のＵＳＢに図３に示すピアトークン１０のＵＳＢ２コネクタ２８を差し込むと、パーソナルコンピュータ１２側からＵＳＢ２インタフェース６２の電源ラインを通じてピアトークン１０に電源供給が行われ、図４に示したピアトークン１０のハードウェアが起動し、図５のデバイス処理プログラム４２がＭＰＵ３２のメモリ領域に読み込まれて実行され、このデバイス処理プログラム４２の実行により、ＵＳＢドライバ５４、ＰＨＳドライバ５０及び無線ＬＡＮ５２が動作状態となる。

【００４６】

ピアトークン１０をパーソナルコンピュータ１２に差し込んだ際にパーソナルコンピュータ１２側にピアトークン１０のデバイスドライバ４４が存在しなかった場合には、図７のようなインストール要求画面４５がパーソナルコンピュータ１２側で表示され、デバイスドライバ４４のインストールを促す。

【００４７】

そこで、ユーザはインストール要求画面４５に続いてアイテム４５－１に示されている「一覧または特定の場所からインストールする」を選択して移行ボタン４５－２を操作すると、パーソナルコンピュータ１２のＵＳＢドライバ６０からピアトークン１０のＵＳＢドライバ５４にインストール要求のためのコマンドが転送され、図８のようにフラッシュメモリ３４からデバイスドライバ４４が読み出され、パーソナルコンピュータ１２のＯＳ５８の処理機能の１つとしてデバイスドライバ４４－１がインストールされる。

【００４８】
ピアトークン１０のデバイスドライバ４４－１がインストールされると、図９のようにデバイスドライバ４４－１によってピアトークン１０から個人認証ライブラリ４８－１がインストールされ、認証画面がパーソナルコンピュータ１２に表示される。

【００４９】
このためユーザは、認証画面の入力枠に対しＩＤとパスワードを入力して認証を要求すると、図２のようにＰＨＳ基地局２０またはホットスポット２２にある無線ＬＡＮのいずれかによる無線回線により認証サーバ２４に対し認証要求が行われ、正しいユーザであれば承認応答が得られる。

【００５０】
このような認証に成功すると、パーソナルコンピュータ１２側のデバイスドライバ４４－１は、図１０のようにピアトークン１０のグループウェア４６をパーソナルコンピュータ１２のＯＳ５８の配下のアプリケーションプログラムであるグループウェア４６－１としてインストールし、これによってグループウェアシステム環境がパーソナルコンピュータ１２側に構築される。

【００５１】
ここで、パーソナルコンピュータ１２はピアトークン１０を保有しているユーザが例えば出張などにより借用した装置であり、ピアトークン１０の差込みにより、借用したパーソナルコンピュータ１２上にユーザ個人のグループウェアシステム環境を個人の認証処理のみをもって簡単に構築することができる。

【００５２】
図１１は、パーソナルコンピュータ１２から本発明のピアトークン１０を外した際の説明図である。パーソナルコンピュータ１２にピアトークン１０を差し込んでグループウェアシステム環境による共有データの送受信や処理を行って作業を終了したならば、グループウェアシステム環境のアプリケーション終了を行った後にピアトークン１０をパーソナルコンピュータ１２から外し、ＵＳＢ２インタフェース６２による接続を切り離す。

【００５３】
このピアトークン１０の切り離しに先立ってグループウェアのアプリケーション終了操作が行われると、パーソナルコンピュータ１２からピアトークン１０に対し終了通知が行われ、ピアトークン１０側で必要な終了処理が行われると同時に、パーソナルコンピュータ１２側にあっては、図１１のようにパーソナルコンピュータ１２側にインストールされているデバイスドライバ４４－１、個人認証ライブラリ４８－１及びグループウェア４６－１のアンインストールが自動的に行われる。

【００５４】
またグループウェアシステム環境の構築で送受信されたデータについては、全てピアトークン１０のフラッシュメモリ３４に保存されている。このため、ピアトークン１０をパーソナルコンピュータ１２から外した場合、ピアトークン１０の差込みで構築した環境は全て削除され、ピアトークン１０によりパーソナルコンピュータ１２を利用しても、使用後にあってはパーソナルコンピュータ１２にピアトークン１０の使用による環境を一切残すことがなく、パーソナルコンピュータ１２の環境をピアトークン１０の使用で侵すことがない。

【００５５】
図１２は、本発明のピアトークン１０を出張先で借りた装置に接続した際の処理手順のフローチャートである。

【００５６】
図２において、ピアトークン１０をステップＳ１でパーソナルコンピュータ１２のＵＳＢ２ポートに接続すると、パーソナルコンピュータ１２にあっては、ステップＳ１０１でＵＳＢ２ポートに対するデバイスの存在を検知し、ピアトークン１０のデバイスドライバを持たない場合には、ステップＳ１０２でデバイスドライバのインストールを行う。

【００５７】

即ち、パーソナルコンピュータ１２は図７のようなインストール要求画面を表示し、このインストール要求画面に対するユーザの操作でデバイスドライバのインストール要求をピアトークン１０に対し行い、これを受けてピアトークン１０は、ステップＳ２でデバイスドライバをパーソナルコンピュータ１２に転送し、デバイスドライバがインストールされて実行される。

【００５８】

次にパーソナルコンピュータ１２側にあっては、インストールされたデバイスドライバの実行で、ステップＳ１０３において認証ライブラリのインストールを行う。即ち、ピアトークン１０に対し認証ライブラリのインストール要求を行い、これを受けてピアトークン１０は、ステップＳ３で個人認証ライブラリの転送を行い、パーソナルコンピュータ１２における認証ライブラリのインストールと実行が行われる。

【００５９】

認証ライブラリが実行されると、ステップＳ１０４で認証画面が表示され、この認証画面に対しユーザはＩＤとパスワードを入力することで、ピアトークン１０に対し認証要求を行う。ピアトークン１０は、ステップＳ４でＰＨＳまたは無線ＬＡＮ経由で認証要求のための送受信を外部の認証サーバとの間で行い、認証サーバから認証結果を受け、ステップＳ５で認証結果をパーソナルコンピュータ１２に通知する。

【００６０】

パーソナルコンピュータ１２にあっては、ステップＳ１０５で認証を取得した場合には、ステップＳ１０６以降の処理に進む。認証が取得できなかった場合には、ステップＳ１１０の処理に進む。認証を取得した場合には、まずステップＳ１０６でピアトークン１０からのグループウェアのインストールを行う。

【００６１】

即ち、ピアトークン１０に対しグループウェアのインストール要求を行い、これを受けてピアトークン１０がステップＳ６でグループウェアの転送を行い、パーソナルコンピュータ１２にグループウェアがインストールされて実行される。

【００６２】

このようにしてパーソナルコンピュータ１２でグループウェアシステム環境が構築されると、ステップＳ１０７で共有ファイルの同期処理を行う。共有ファイルの同期処理は、グループウェアシステム環境に属している他のピア装置との間で共有データが同じになるように差分データの転送によるマージ処理を行う。

【００６３】

この共有ファイルの同期処理に伴う他のピア装置との間のやり取りのため、ピアトークン１０にあっては、ステップＳ７のようにＰＨＳまたは無線ＬＡＮによる転送処理を行う。

【００６４】

続いてステップＳ１０８で、グループウェアシステム環境の構築の下にピアツーピアによるグループウェアの運用が行われる。このグループウェアの運用における他のピア装置との間のデータのやり取りについても、ピアトークン１０はステップＳ８のように、ＰＨＳまたは無線ＬＡＮによる転送処理を行う。

【００６５】

ステップＳ１０９でグループウェアの終了が判別されると、ステップＳ１１０で終了通知をピアトークン１０に対し行った後、ステップＳ１１１でピアトークン１０の差込みによりインストールしたデバイスドライバ、個人認証ライブラリ及びグループウェアのアンインストールを自動的に行う。

【００６６】

またピアトークン１０にあっては、パーソナルコンピュータ１２からの終了通知を受けて、ステップＳ９でポート切り離しに伴う電源断に対する終了処理を行う。最終的に、パーソナルコンピュータ１２からピアトークン１０をステップＳ１０で抜き外し、これによってパーソナルコンピュータ１２にあっては、ステップＳ１１２でＵＳＢ２ポートのデバイス存在を認識してＵＳＢの処理を終了させる。

【００６７】
図１３は、図１２のグループウェアシステム環境を構築した際のパーソナルコンピュータ１２のステップＳ１０７における共有ファイル同期処理の詳細を示したフローチャートである。

【００６８】
図１３において、共有ファイル同期処理は、ステップＳ１０１でピアトークン１０に対し保存ファイルの更新情報を要求する。これを受けてピアトークン１０にあっては、ステップＳ１でファイル名と更新情報をパーソナルコンピュータ１２に応答する。

【００６９】
続いてステップＳ１０２で、パーソナルコンピュータ１２はグループウェアに属する他のピア装置に対し、ピアトークン１０に保存している共有ファイルの更新情報を要求する。これを受けてピアトークン１０は、ステップＳ２でＰＨＳまたは無線ＬＡＮで他のピア装置に対し共有ファイルの更新情報をアクセスして結果を通知する。

【００７０】
続いてステップＳ１０３で、ピアトークン１０と他のピア装置とで更新日の異なるファイルについて他のピア装置に対し差分データの転送を要求し、これを受けてピアトークン１０は、ステップＳ３でＰＨＳまたは無線ＬＡＮで他のピア装置にアクセスし、差分データを取得する。

【００７１】
このため、ステップＳ１０４でピアトークン１０に対し差分データのマージによるファイル更新を指示する。これを受けてピアトークン１０は、ステップＳ４で他のピア装置から受信した差分データを対応する保存ファイルとマージすることでファイル更新を行う。

【００７２】
なおステップＳ４の差分データのマージはピアトークン１０側で行わず、パーソナルコンピュータ１２側で行って、結果をピアトークン１０のメモリに保存するようにしてもよい。

【００７３】
このようにピアトークン１０をパーソナルコンピュータ１２に差し込んでグループウェアシステム環境を構築すると、最初にピアトークン１０に保存している共有データの同期処理が行われるため、その後のグループウェアシステム環境でのファイル利用は常に最新のファイルを対象に行うことができる。

【００７４】
図１４は、グループウェアシステム環境がピアトークン１０の差込みで構築されたパーソナルコンピュータ１２におけるファイルアクセスの処理手順のフローチャートである。

【００７５】
まずステップＳ１０１でパーソナルコンピュータ１２側でのファイルオープンが行われると、このファイルオープン要求がピアトークン１０に伝えられ、ステップＳ１で該当ファイルをフラッシュメモリ３４から読み出して転送し、ステップＳ１０２で必要とするファイル処理を行う。

【００７６】
またステップＳ１０３で、オープンしたファイルのクローズが判別されると、ステップＳ１０４でファイルをピアトークン１０に転送し、フラッシュメモリ３４に格納する。

【００７７】
ここで、ステップＳ１０２のファイル処理においてオープンしたファイルについて新たなデータを追加するなどしてファイル容量が増加する場合があり、ファイルオープン時にはメモリ容量が十分であったものが、ファイルクローズに伴うメモリ格納時にはフラッシュメモリ３４のメモリ容量が不足する場合がある。

【００７８】
そこでピアトークン１０にあっては、ステップＳ１０４からファイルクローズに伴うファイル転送を受けると、ステップＳ２でメモリ容量が不足するか否かチェックする。もしメ

モリ容量が不足した場合にはステップＳ３に進み、図５のデータ領域５５に格納しているファイルリスト５６の末尾のファイルｎに対応したファイルｎデータを取得し、ステップＳ４で他のピア装置例えば図２におけるパーソナルコンピュータ１２に対し近隣となるピア装置１４－４に転送して保存する。

【００７９】

続いてステップＳ５でファイルｎの実データを消去し、ここに他のピア装置の保存を示すリンク情報を格納する置き換えを行う。このようにファイルｎのデータを消去してそのリンク情報に置き換えることで、リンク情報の必要容量はごく少ないことから実データ域５７に空き容量を確保できる。

【００８０】

そしてステップＳ６で、ファイルクローズに伴い転送された使用済みファイルをファイルリスト５６の先頭位置に格納する。もちろんファイルリストの末尾のファイルを１つ、他のピア装置に転送して実データを消去してもなおメモリ容量が不足する場合には、再度、末尾のファイルを削除してメモリ空き容量を確保する処理を、メモリ容量の不足が解消するまで繰り返すことになる。

【００８１】

このため、ピアトークン１０のメモリ容量に制約があっても、実データを他のピア装置に保存してそのリンク情報をピアトークン１０に保存することで、ピアトークン１０におけるメモリ容量不足の影響を受けることなく、グループウェアシステム環境において使用している共有データの実質的な保存と利用が実現できる。

【００８２】

図１５は、本発明のピアトークンを携帯電話に接続して、交通機関改札のゲートシステムや自動販売機の制御処理を行う他の実施形態の説明図である。

【００８３】

図１５において、携帯電話６１は、図２の実施形態におけるパーソナルコンピュータ１２の場合と同様、ＵＳＢ２ポートに相当するデバイスポートを持っており、ピアトークン１０の差込みで電源供給と同時にデータ転送を可能とする。

【００８４】

ピアトークン１０のフラッシュメモリには、例えば図１６のメモリマップ６８に示すように、図５のメモリマップ４０の内容に加えて新たに、ゲート処理プログラム７０と自動販売機処理プログラム７２が格納されており、ピアトークン１０の携帯電話６１に対する差込みでインストールされてアプリケーションプログラムとして動作させることができる。

【００８５】

図１７は、ゲートシステム６４を対象とした本発明のピアトークンと携帯電話の処理手順のフローチャートである。

【００８６】

図１７において、携帯電話６４にピアトークン１０を差し込んだ状態で交通機関の改札ゲートを通過しようとすると、ゲートの通信可能領域に入ったときにピアトークン１０はステップＳ１でゲートを認識し、ステップＳ２でゲート検知通知を携帯電話６１に送る。

【００８７】

これを受けて携帯電話６１側は、ステップＳ１０１でゲートイン要求をピアトークン１０に行い、ステップＳ３でＰＨＳまたは無線ＬＡＮによる無線送受信でゲートシステム６４に対しゲート要求を送り、応答結果を受信して携帯電話６４に返す。

【００８８】

このゲートイン要求に対し、ゲートシステム６４にあっては、改札ゲートを開くか、あるいはユーザの通過に対しロックを解除する。ゲートシステム６４からの応答情報には入場駅を示す入場情報が含まれていることから、ステップＳ１０２で入場情報を保持する。

【００８９】

このようにして改札ゲートに入った後は、ステップＳ４でピアトークン１０は再度、ゲート認識をチェックしており、利用者が到着駅のゲートから出ようとする際にゲート認識を

行って、ステップＳ５でゲート検知通知を携帯電話６１側に送る。これを受けて携帯電話６１は、ステップＳ１０３でゲートアウト要求をピアトークン１０のステップＳ６の無線送受信を介してゲートシステムに対し行い、このゲートアウト要求を受けてゲートシステム６４は、計算された料金データを応答する。

【００９０】

料金データを受けた携帯電話６１側にあっては、ステップＳ１０４で料金精算処理を行う。この料金精算処理は、予め保存しているプリペイド料金からの減額あるいは銀行口座から引き出している電子マネーの支払いなど、適宜の精算処理が行われる。

【００９１】

精算処理の結果はステップＳ７の無線送受信を通じてゲートシステム６４に通知され、精算確認応答を受けて、ステップＳ１０５で処理を終了し、一方、ゲートシステム６４にあっては精算確認に伴いゲート開あるいはゲートロック解除を行って、ユーザのゲート通過を可能とする。

【００９２】

図１８は、図１５の自動販売機６６を対象とした本発明のピアトークンと携帯電話における処理手順のフローチャートである。携帯電話６４に本発明のピアトークン１０を差し込んだ状態でユーザが自動販売機の前に立つと、ピアトークン１０はステップＳ１で自動販売機からの電波を受信して認識し、ステップＳ２で自動販売機の検知通知を携帯電話６１側に行う。

【００９３】

これに伴いユーザは、携帯電話６１を使用してステップＳ１０１で商品の購入要求を行う。例えば携帯電話６１の画面上に商品に選択画像が表示され、ユーザは購入したい商品を選択して実行要求することで、商品の購入要求がピアトークン１０のステップＳ３の無線送受信を通じて自動販売機に伝えられ、自動販売機より請求代金がピアトークン１０を介して携帯電話６１側に送られる。

【００９４】

そこで、ステップＳ１０２において購入代金の精算処理を行うと、プリペイド料金からの購入代金の残額あるいは銀行口座から引き落とした電子マネーの支払いがステップＳ４の無線送受信を通じて行われ、自動販売機から精算確認応答が得られると、ステップＳ１０３で終了処理を行う。

【００９５】

このような図１７における交通機関のゲート処理や図１８の自動販売機処理における代金精算結果はピアトークン１０のフラッシュメモリに保存され、ユーザが自分のパーソナルコンピュータの設置場所に戻ってピアトークンを差し込むと、ピアトークン１０に保存されている精算情報が自分のパーソナルコンピュータ側に転送されて自動的に編集され、ユーザの資産情報にマージするなどの処理を行わせることができる。

【００９６】

なお、グループウェアシステム環境における共有データの使い方として、自分のパーソナルコンピュータの実体データはサーバに保管しておき、サーバのファイル管理に使用しているネットワーク設定、各種アカウントなどのレジストリ情報をピアトークンに登録し、本発明のピアトークンを別のパーソナルコンピュータに挿入してレジストリ情報に基づくサーバからの共有ファイルの転送を行わせることで、本発明のピアトークンを別のパーソナルコンピュータに挿入すると同時に、自分が通常使用している作業環境を直ちに実現することができる。

【００９７】

また上記の実施形態は、ピアトークンに格納するアプリケーションとしてグループウェアプログラム、ゲート処理プログラム、自動販売機処理プログラムを例に取るものであったが、本発明はこれに限定されず、無線回線を利用して他の装置との間でデータのやり取りを行う適宜のアプリケーションをピアトークンに格納してパーソナルコンピュータやＰＤＡ、更には携帯電話に差し込むことで、差込み先の装置にアプリケーションプログラム環

境を構築して利用することができる。

【００９８】

また本発明は、その目的と利点を損なうことのない適宜の変形を含み、更に実施形態に示した数値による限定は受けない。

【００９９】

ここで本発明の特徴をまとめると次の付記のようになる。

（付記）

（付記１）

電源供給とデータ転送が可能な情報処理装置のデバイスポートに対し着脱自在なポートコネクタと、

外部装置に対し無線回線により情報を送受する第１無線通信部と、

外部装置に対し前記第１無線通信部とは異なる無線回線を使用して情報を送受する第２無線通信部と、

デバイスドライバ、ポートドライバ、個人認証ライブラリ、任意のアプリケーションプログラム、第１無線通信用ドライバ及び第２無線通信用ドライバを格納した不揮発メモリと、

前記ポートコネクタを情報処理装置のデバイスポートに接続した際に起動し、前記情報端末装置からの最初のデバイスアクセスに対し前記デバイスドライバを転送してインストールさせ、インストールされた前記デバイスドライバにより前記個人認証ライブラリをインストールさせて個人認証を行わせ、個人認証に成功した場合に前記アプリケーションプログラムをインストールして実行させ、前記認証ライブラリ及びアプリケーションプログラムの実行による外部装置とのアクセスを前記第１又は第２無線通信用ドライバにより行わせ、アプリケーションの終了時には前記デバイスドライバ、個人認証ライブラリ及びアプリケーションプログラムをアンインストールさせるデバイス処理部と、

を備えたことを特徴とする情報処理デバイス。（１）

【０１００】

（付記２）

付記１記載の情報処理デバイスに於いて、デバイス本体は持ち運び自在なキー型であることを特徴とする情報処理デバイス。

【０１０１】

（付記３）

付記１記載の情報処理デバイスに於いて、前記デバイスポートはＵＳＢ２ポートであり、前記ポートドライバはＵＳＢ２ドライバであることを特徴とする情報処理デバイス。

【０１０２】

（付記４）

付記１記載の情報処理デバイスに於いて、前記第１無線通信部はＰＨＳ無線回線を使用するＰＨＳ通信部であり、前記第２無線通信部は無線ＬＡＮを使用する無線ＬＡＮ通信部であることを特徴とする情報処理デバイス。

【０１０３】

（付記５）

付記１記載の情報処理デバイスに於いて、前記アプリケーションプログラムは複数の情報処理装置でデータを共有するピアツーピア型のグループウェア処理プログラムであることを特徴とする情報処理デバイス。（２）

【０１０４】

（付記６）

付記５記載の情報処理デバイスに於いて、前記アプリケーションプログラムがグループウェア処理プログラムの場合、前記個人認証ライブラリは前記第１又は第２無線通信部により外部の認証サーバに接続して認証処理を実行させることを特徴とする情報処理デバイス。

【０１０５】

（付記７）
付記１記載の情報処理デバイスに於いて、前記不揮発メモリに自己の情報処理装置で使用しているファイルをサーバに格納したことを示すディレクトリ情報を登録し、前記アプリケーションプログラムは、他の情報処理装置の差込み時に、前記レジストリ情報により前記サーバからファイルを取得して前記自己の情報処理装置の作業環境を構築することを特徴とする情報処理デバイス。（３）

【０１０６】
（付記８）
電源供給とデータ転送が可能な情報処理装置のデバイスポートに対し着脱自在なポートコネクタと、外部装置に対し無線回線により情報を送受する第１無線通信部と、外部装置に対し前記第１無線通信部とは異なる無線回線を使用して情報を送受する第２無線通信部と、デバイスドライバ、ポートドライバ、個人認証ライブラリ、任意のアプリケーションプログラム、第１無線通信用ドライバ及び第２無線通信用ドライバを格納した不揮発メモリとを備えたデバイスの情報処理方法に於いて、
前記ポートコネクタを情報処理装置のデバイスポートに接続した際に起動し、前記情報端末装置からの最初のデバイスアクセスに対し前記デバイスドライバを転送してインストールさせる起動ステップと、
インストールされた前記デバイスドライバにより前記個人認証ライブラリをインストールさせて個人認証を行わせる個人認証ステップと、
個人認証に成功した場合に前記アプリケーションプログラムをインストールして実行させる実行ステップと、
前記認証ライブラリ及びアプリケーションプログラムの実行による外部装置とのアクセスを前記第１又は第２無線通信用ドライバにより行わせる通信ステップと、
アプリケーションプログラムの終了時に前記デバイスドライバ、個人認証ライブラリ及びアプリケーションプログラムをアンインストールさせるアンインストールステップと、
を備えたことを特徴とする情報処理方法。（４）

【０１０７】
（付記９）
電源供給とデータ転送が可能な情報処理装置のデバイスポートに対し着脱自在なポートコネクタと、外部装置に対し無線回線により情報を送受する第１無線通信部と、外部装置に対し前記第１無線通信部とは異なる無線回線を使用して情報を送受する第２無線通信部と、デバイスドライバ、ポートドライバ、個人認証ライブラリ、任意のアプリケーションプログラム、第１無線通信用ドライバ及び第２無線通信用ドライバを格納した不揮発メモリとを備えたデバイスのコンピュータに、
前記ポートコネクタを情報処理装置のデバイスポートに接続した際に起動し、前記情報端末装置からの最初のデバイスアクセスに対し前記デバイスドライバを転送してインストールさせる起動ステップと、
インストールされた前記デバイスドライバにより前記個人認証ライブラリをインストールさせて個人認証を行わせる認証ステップと、
個人認証に成功した場合に前記アプリケーションプログラムをインストールして実行させる実行ステップと、
前記認証ライブラリ及びアプリケーションプログラムの実行による外部装置とのアクセスを前記第１又は第２無線通信用ドライバにより行わせる通信ステップと、
アプリケーションプログラムの終了時に前記デバイスドライバ、個人認証ライブラリ及びアプリケーションプログラムをアンインストールさせるアンインストールステップと、
を実行させることを特徴とするプログラム。（５）

【０１０８】
【発明の効果】
以上説明してきたように本発明によれば、キー型に形成された小型の情報処理デバイスを例えば出張先で使用することのできるパーソナルコンピュータのデバイスポートに差し込

むだけで、個人認証画面が自動的に立ち上がり、個人認証を済ませた後はグループウェアなどのアプリケーション画面が立ち上がり、外部との送受信を含む作業をすぐ始めることができる。

【０１０９】

また外部との通信に使用する無線通信機能がＰＨＳと無線ＬＡＮにより二重化されており、使用場所の無線環境に対応して有効な側に自動切替して外部に確実にアクセスすることができる。

【０１１０】

更に、情報処理デバイスの差込みによるアプリケーションの実行で使用されたデータは全てデバイス側の不揮発メモリに保存され、また情報処理デバイスを抜いて処理を終えると、パーソナルコンピュータなどの差込み側の装置にはインストールしたプログラムやドライバは全てアンインストールされて残ることがなく、差込み先の装置の環境を全く侵すことなく、本発明の情報処理デバイスの差込みによるアプリケーション環境の利用が実現できる。

【図面の簡単な説明】

【図１】本発明の原理説明図

【図２】本発明が適用されたシステム環境の説明図

【図３】本発明によるキー型ピアトークンの外観の説明図

【図４】本発明によるピアトークンのハードウェア構成のブロック図

【図５】図４の不揮発メモリの格納内容となるメモリマップの説明図

【図６】本発明のピアトークンを使用先となるパーソナルコンピュータに接続した起動時の説明図

【図７】ピアトークンの接続による使用先となるパーソナルコンピュータのインストール要求画面の説明図

【図８】図６に続いて使用先となるパーソナルコンピュータにデバイスドライバがインストールされた説明図

【図９】図８に続いて使用先となるパーソナルコンピュータに個人認証ライブラリがインストールされた説明図

【図１０】図９に続いて使用先となるパーソナルコンピュータにグループウェアがインストールされた説明図

【図１１】使用先となるパーソナルコンピュータのデバイスポートから本発明のピアトークンを外した際の説明図

【図１２】本発明のピアトークンを使用先となるパーソナルコンピュータに接続した際の処理手順のフローチャート

【図１３】共有ファイル同期処理における本発明のピアトークンと使用先となるパーソナルコンピュータの処理手順のフローチャート

【図１４】ファイルアクセスにおける本発明のピアトークンと使用先となるパーソナルコンピュータの処理手順のフローチャート

【図１５】本発明のピアトークンを携帯電話に接続して交通機関改札のゲートシステムや自動販売機の制御処理を行う実施形態の説明図

【図１６】図６のピアトークンにおける不揮発メモリのメモリマップ説明図

【図１７】ゲートシステムを対象とした本発明のピアトークンと携帯電話の処理手順のフローチャート

【図１８】自動販売機を対象とした本発明のピアトークンと携帯電話の処理手順のフローチャート

【符号の説明】

１０：ピアトークン（情報処理デバイス）

１２：パーソナルコンピュータ

１４－１～１４－４：ピア装置

１５：ＬＡＮ

１６：インターネット

１８：プロキシサーバ

２０：ＰＨＳ基地局

２２：ホットスポット（無線ＬＡＮ）

２４：認証サーバ

２６：デバイス本体

２８：ＵＳＢ２コネクタ

３０，６２：ＵＳＢ２インタフェース

３２：ＭＰＵ（プロセッサ）

３４：フラッシュメモリ（不揮発メモリ）

３６：ＰＨＳ送受信部

３８：無線ＬＡＮ送受信部

４０，６８：メモリマップ

４２：デバイス処理プログラム（トークンＯＳ）

４４：デバイスドライバ

４５：インストール要求画面

４６：グループウェア

４８：個人認証ライブラリ

５０：ＰＨＳドライバ

５２：無線ＬＡＮドライバ

５４，６０：ＵＳＢドライバ

５５：データ領域

５６：ファイルリスト

５７：実データ域

５８：使用先となるパーソナルコンピュータＯＳ

６１：携帯電話

６４：ゲートシステム

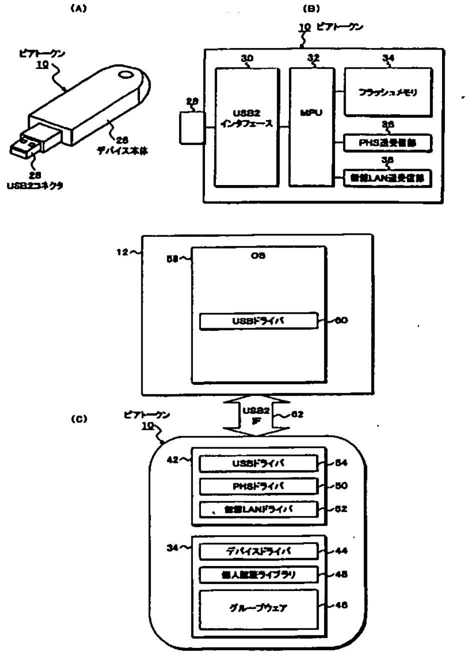
６６：自動販売機

７０：ゲート処理プログラム

７２：自動販売機処理プログラム

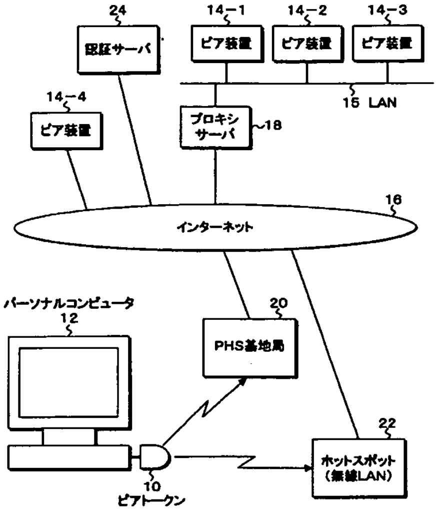
【図１】

本発明の原理説明図



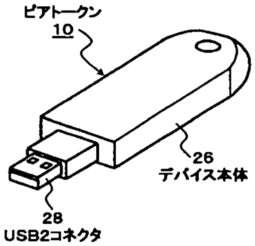
【図２】

本発明が適用されたシステム環境の説明図



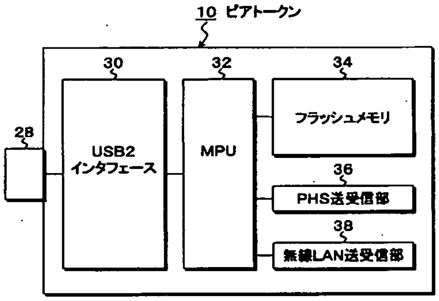
【図３】

本発明によるキー一型ピアトークンの外観の説明図



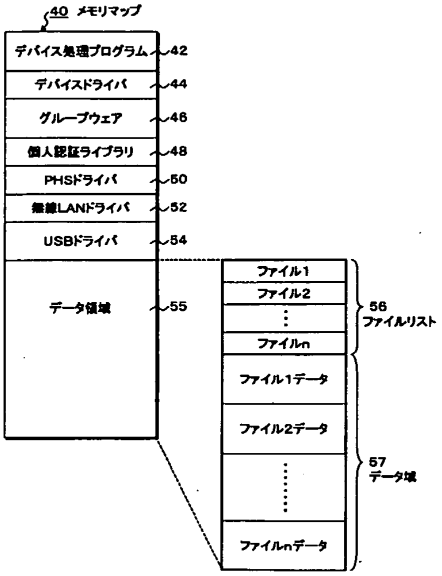
【図４】

本発明によるピアトークンのハードウェア構成のブロック図



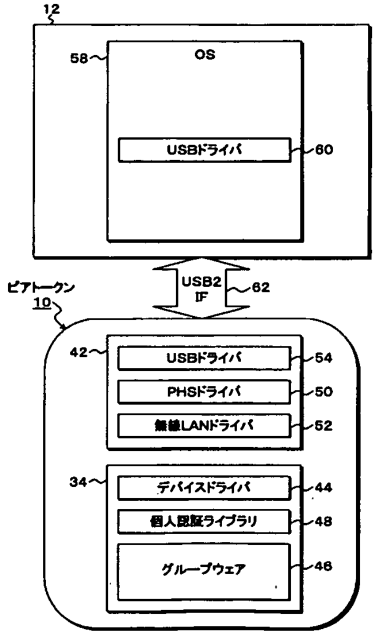
【図５】

図4の不揮発メモリの格納内容となるメモリマップの説明図



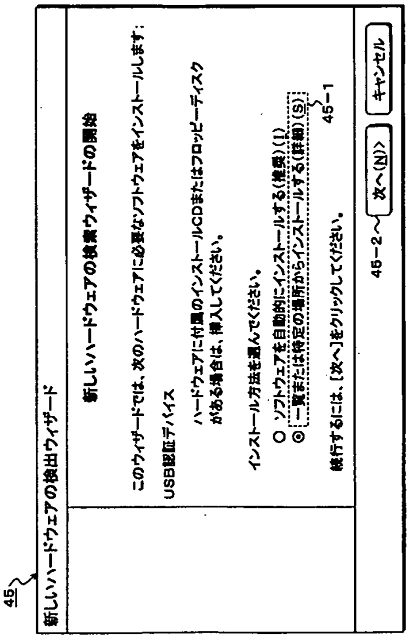
【図６】

本発明のピアトークンを使用先のパーソナルコンピュータに接続した起動時の説明図



【図７】

ピアトークンの接続による使用先のパーソナルコンピュータのインストール要求画面の説明図



新しいハードウェアの検出ウィザード

新しいハードウェアの検索ウィザードの開始

このウィザードでは、次のハードウェアに必要なソフトウェアをインストールします：

USB認証デバイス

ハードウェアに付属のインストールCDまたはフロッピーディスクがある場合は、挿入してください。

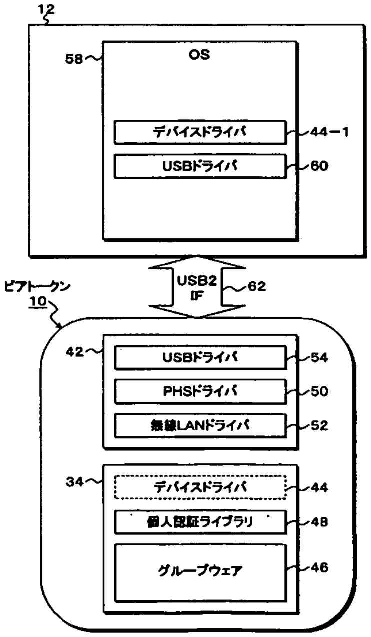
インストール方法を選んでください。

○ ソフトウェアを自動的にインストールする(推奨)(I)
◉ 一覧または特定の場所からインストールする(詳細)(S)

続行するには、[次へ]をクリックしてください。

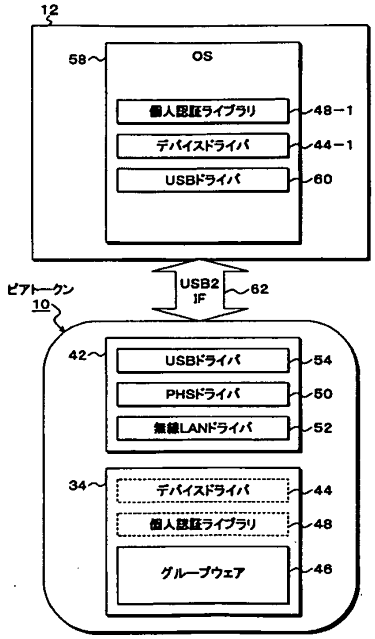
【図８】

図6に続いて使用先のパーソナルコンピュータにデバイスドライバがインストールされた説明図



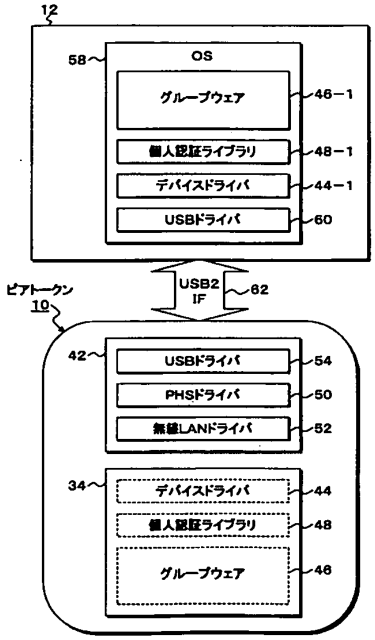
【図９】

図8に続いて使用先のパーソナルコンピュータに個人認証ライブラリがインストールされた説明図



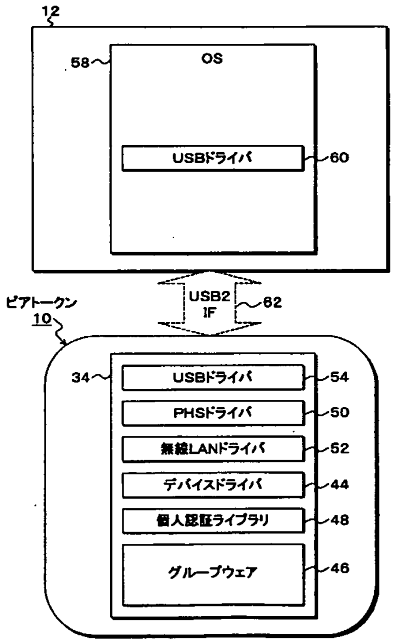
【図１０】

図9に続いて使用先のパーソナルコンピュータにグループウェアがインストールされた説明図



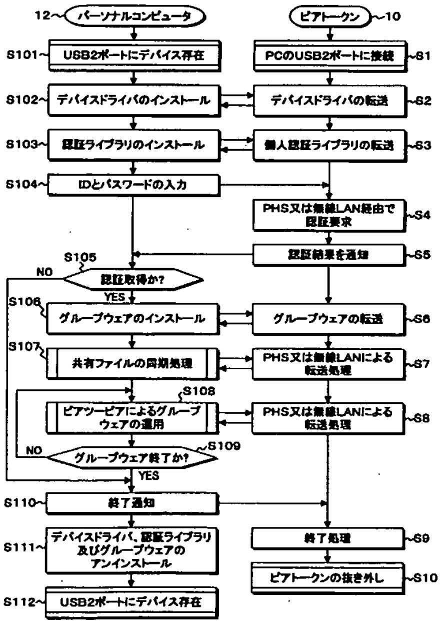
【図１１】

使用先のパーソナルコンピュータのデバイスポートから本発明のピアトークンを外した際の説明図



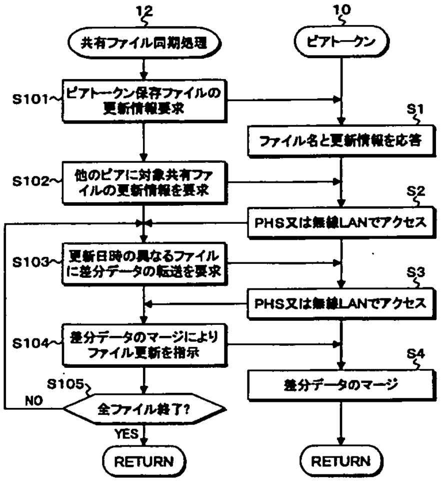
【図１２】

本発明のピアトークンを使用先のパーソナルコンピュータに接続した際の処理手順のフローチャート



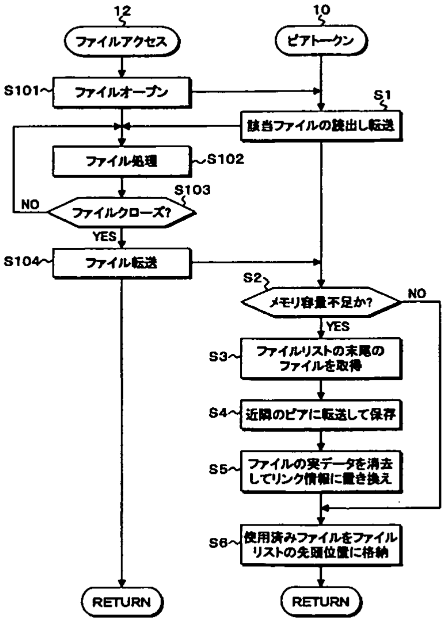
【図１３】

共有ファイル同期処理における本発明のピアトークンと使用先のパーソナルコンピュータの処理手順のフローチャート


12
10
共有ファイル同期処理
ピアトークン
S101
ピアトークン保存ファイルの更新情報要求
S1
ファイル名と更新情報を応答
S102
他のピアに対象共有ファイルの更新情報を要求
S2
PHS又は無線LANでアクセス
S103
更新日時の異なるファイルに差分データの転送を要求
S3
PHS又は無線LANでアクセス
S104
差分データのマージによりファイル更新を指示
S4
差分データのマージ
S105
NO
全ファイル終了?
YES
RETURN
RETURN

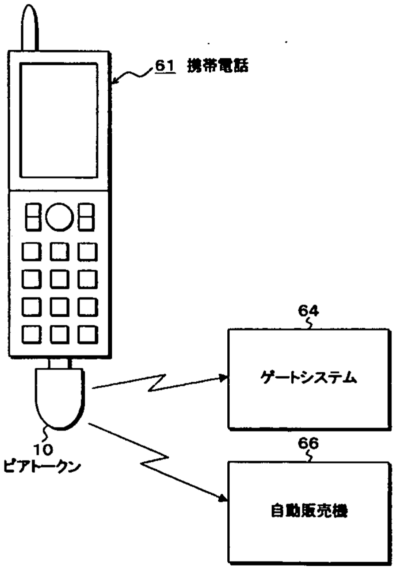
【図１４】

ファイルアクセスにおける本発明のピアトークンと使用先のパーソナルコンピュータの処理手順のフローチャート



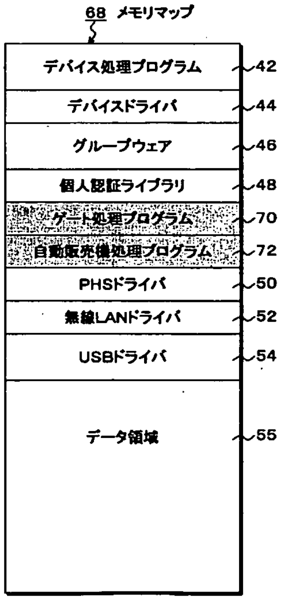
【図１５】

本発明のピアトークンを携帯電話に接続して交通機関改札のゲートシステムや自動販売機の制御処理を行う実施形態の説明図



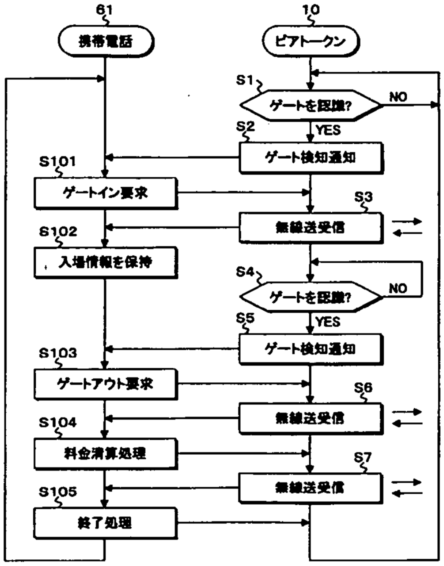
【図１６】

図６のピアトークンにおける不揮発メモリのメモリマップ説明図



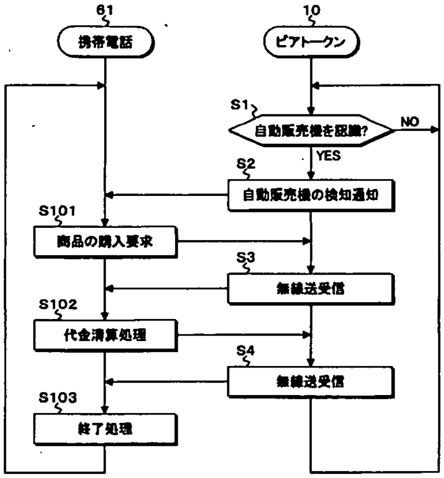
【図１７】

ゲートシステムを対象とした本発明のピアトークンと携帯電話の処理手順のフローチャート



【図１８】

自動販売機を対象とした本発明のピアトークンと携帯電話の処理手順のフローチャート



フロントページの続き

(51)Int.Cl.^{7}	FI	テーマコード（参考）
	G06F 9/06 660E	

Fターム(参考) 5B014 FA14
5B076 AB20 BA05 BA10 BB12 BB18 FB01
5B085 AA04 AE02 AE12 AE23 BE01 BE04 BG01 BG02 BG07

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
20 December 2001 (20.12.2001)

PCT

(10) International Publication Number
WO 01/96990 A2

(51) International Patent Classification⁷: G06F 1/00

(21) International Application Number: PCT/EP01/06816

(22) International Filing Date: 15 June 2001 (15.06.2001)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
09/594,456 15 June 2000 (15.06.2000) US

(71) Applicant: RAINBOW TECHNOLOGIES, B.V. [NL/NL]; Oliphanteweg 10, NL-1397 Le Rotterdam (NL).

(72) Inventors: **ABBOTT, Shawn, D.**; 305 Pinnacle Ridge Place, RR12, Calgary, Alberta T3E 6W3 (CA). **ANDERSON, Allan, D.**; 11158 Bertha Place, Cerritos, CA 90703 (US). **GODDING, Patrick, N.**; 22665 Shady Grove Circle, Lake Forest, CA 92630 (US). **PUNT, Maarten, G.**; 24942 Paseo Arboleda, Lake Forest, CA 92630 (US). **SOTOODEH, Mehdi**; 17 Paloma Drive, Mission Viejo, CA 92692 (US).

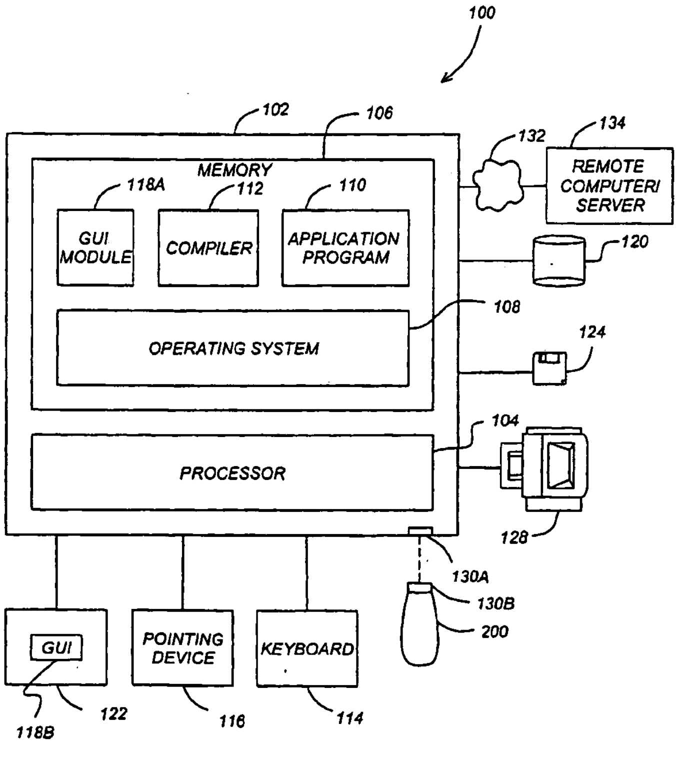
(74) Agents: **SMITH, Samuel, Leonard** et al.; J.A. Kemp & Co., 14 South Square, Gray's Inn, London WC1R 5JJ (GB).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW.

(84) Designated States *(regional)*: ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European

[Continued on next page]

(54) Title: USB-COMPLIANT PERSONAL KEY USING A SMARTCARD PROCESSOR AND A SMARTCARD READER EMULATOR



(57) **Abstract:** A compact, self-contained, personal key is disclosed. The personal key comprises a USB-compliant interface releaseably coupleable to a host processing device operating under command of an operating system; a smartcard processor having a smartcard processor-compliant interface of communicating according to a smartcard input and output protocol; and an interface processor, communicatively coupled to the USB-compliant interface and to the smartcard processor-compliant interface, the interface processor implementing a translation module for interpreting USB-compliant messages into smartcard processor-compliant messages and for interpreting smartcard processor-compliant messages into USB-compliant messages.

WO 01/96990 A2

patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published:

— *without international search report and to be republished upon receipt of that report*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

USB-COMPLIANT PERSONAL KEY USING A SMARTCARD PROCESSOR AND A SMARTCARD READER EMULATOR

CROSS-REFERENCE TO RELATED APPLICATIONS

This application is a continuation-in-part of U.S. Patent Application No. 09/449,159, filed November 24, 1999, by Shawn D. Abbott, Bahram Afghani, Mehdi Sotoodeh, Norman L. Denton III, and Calvin W. Long, and entitled "USB-Compliant Personal Key with Integral Input and Output Devices," which is a continuation-in-part of U.S. Patent Application No. 09/281,017, filed March 30, 1999 by Shawn D. Abbott, Bahram Afghani, Allan D. Anderson, Patrick N. Godding, Maarten G. Punt, and Mehdi Sotoodeh, and entitled "USB-Compliant Personal Key," which claims benefit of U.S. Provisional Patent Application No. 60/116,006, filed January 15, 1999 by Shawn D. Abbott, Barham Afghani, Allan D. Anderson, Patrick N. Godding, Maarten G. Punt, and Mehdi Sotoodeh, and entitled "USB-Compliant Personal Key," all of which applications are hereby incorporated by reference herein.

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to computer peripherals, and in particular to an inexpensive USB-compliant personal key that is compatible with existing smartcard processors, drivers, and instruction sets.

2. Description of the Related Art

In the last decade, the use of personal computers in both the home and in the office have become widespread. These computers provide a high level of functionality to many people at a moderate price, substantially surpassing the performance of the large mainframe computers of only a few decades ago. The trend is further evidenced by the increasing popularity of laptop and notebook computers, which provide high-performance computing power on a mobile basis.

The widespread availability of personal computers has had a profound impact on interpersonal communications as well. Only a decade ago, telephones or fax machines offered virtually the only media for rapid business communications. Today, a growing number of businesses and individuals communicate via electronic mail (e-mail). Personal computers have also been instrumental in the emergence of the Internet and its growing use as a medium of commerce.

While certainly beneficial, the growing use of computers in personal communications, commerce, and business has also given rise to a number of unique challenges. These challenges include the prevention of unauthorized use of software, ensuring the security of e-mail and other electronic communications, as well as Internet commerce.

Smartcards represent a longstanding attempt to deal with at least some of the foregoing challenges. Substantial resources have been made in the design and development of smartcards, smartcard readers, and the associated reader/smartcard drivers which allow computer applications to interface with the smartcard to perform security and data storage functions. Even so, smartcards have not enjoyed widespread popularity. Smartcard readers are relatively expensive, and not widely available. Further, the lack of uniform smartcard/smartcard reader physical interface standards have resulted in smartcard/smartcard reader physical interface compatibility problems, many of which remain unresolved.

USB-compliant personal keys, such as that which is disclosed in co-pending and commonly assigned U.S. Patent Application Nos. 09/449,159 and 09/281,017, described above, offer the benefit of smartcard functionality in a universally accepted USB form factor. The Universal Serial Bus (USB) is a connectivity standard developed by computer and telecommunication industry members for interfacing computers and peripherals. USB-compliant devices allow the user to install and hot-swap devices without long installation procedures and reboots, and features a 127 device bus capacity, dual-speed data transfer, and can provide limited power to devices attached on the bus. Because the USB connectivity standard is rapidly becoming available on most personal computers, it offers a standard, widely available physical interface, the unavailability of which has prevented smartcards from achieving widespread acceptance.

While smartcards have not enjoyed widespread popularity in the United States, they are widely accepted in Europe. Hence, many software applications and drivers have been developed for existing smartcard-based devices and their readers. Unfortunately, smartcard interface protocols such as those described in ISO 7816 are incompatible with the USB protocols used in the above-described devices. This incompatibility has led to two unfortunate consequences. First, to comply with USB interface protocol requirements, current USB-compliant personal keys utilize special purpose processors, instead of the low cost, limited capability processors currently available for smartcards. This increases the cost of the USB-compliant personal key, making widespread acceptance more difficult. Also, because each USB-compatible personal key may use a different processor (and different instruction sets), users may require different device drivers for different personal keys. This too represents another barrier to widespread acceptance of the personal key.

From the foregoing, it is apparent that there is a need for a USB-compliant personal key that is usable with legacy personal identification devices, such as processors having smartcard processors and/or those complying with the ISO 7816. There is also a need for a USB-compliant personal key that makes maximum use of existing smartcard protocols, software and devices wherever possible, and which retain at least a limited compatibility with existing devices designed to interface with smartcards. The present invention satisfies that need.

SUMMARY OF THE INVENTION

The present invention satisfies all of these needs with a personal key in a form factor that is compliant with a commonly available I/O interface such as the Universal Serial Bus (USB) and at the same time, usable with existing smartcard software applications. The personal key comprises a USB-compliant interface releaseably coupleable to a host processing device operating under command of an operating system; a smartcard processor having a smartcard processor-compliant interface for communicating according to a smartcard input and output protocol; and an interface processor, communicatively coupled to the USB-compliant interface and to the smartcard processor-compliant interface, the interface processor implementing a translation module for interpreting USB-compliant messages into smartcard processor-compliant messages and for interpreting smartcard processor-compliant messages into USB-compliant messages.

In one embodiment, the method comprises the steps of accepting a message comprising a smartcard reader command selected from a smartcard reader command set from a host computer operating system in a virtual smartcard reader; packaging the message for transmission via a USB-compliant interface according to a first message transfer protocol; transmitting the packaged message to a personal key communicatively coupled to the USB-compliant interface; receiving the packaged message in the personal key; unpackaging the message in the personal key to recover the smartcard reader command; translating the smartcard reader command into a smartcard command within the personal key; and providing the smartcard command to the smartcard processor.

The present invention is well suited for controlling access to network services, or anywhere a password, cookie, digital certificate, or smartcard might otherwise be used, including:

- Remote access servers, including Internet protocol security (IPSec), point to point tunneling protocol (PPTP), password authentication protocol (PAP), challenge handshake authentication protocol (CHAP), remote access dial-in user service (RADIUS), terminal access controller access control system (TACACS);
- Providing Extranet and subscription-based web access control, including hypertext transport protocol (HTTP), secure sockets layer (SSL);

- Supporting secure online banking, benefits administration, account management;
- Supporting secure workflow and supply chain integration (form signing);
- Preventing laptop computer theft (requiring personal key for laptop operation);
- Workstation logon authorization;
- Preventing the modification or copying of software;
- Encrypting files;
- Supporting secure e-mail, for example, with secure multipurpose Internet mail extensions (S/MIME), and open pretty good privacy (OpenPGP)
- Administering network equipment administration; and
- Electronic wallets, with, for example, secure electronic transaction (SET, MilliCent, eWallet)

BRIEF DESCRIPTION OF THE DRAWINGS

Referring now to the drawings in which like reference numbers represent corresponding parts throughout:

FIG. 1 is a diagram showing an exemplary hardware environment for practicing the present invention;

FIG. 2 is a block diagram of a personal key communicatively coupled to a host computer;

FIG. 3 is a block diagram of a personal key with a smartcard processor communicatively coupled to a host computer; and

FIGs. 4A-4D are flow charts presenting exemplary method steps that can be used to practice the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

In the following description, reference is made to the accompanying drawings which form a part hereof, and which is shown, by way of illustration, several embodiments of the present invention. It is understood that other embodiments may be utilized and structural changes may be made without departing from the scope of the present invention.

FIG. 1 illustrates an exemplary computer system 100 that could be used to implement the present invention. The host computer 102 comprises a processor 104 and a memory, such as random access memory (RAM) 106. The host computer 102 is operatively coupled to a display 122, which presents images such as windows to the user on a graphical user interface 118B. The host computer 102 may be coupled to other devices, such as a keyboard 114, a mouse device 116, a printer 128, etc. Of course, those skilled in the art will recognize that any combination of the above components, or any number of different components, peripherals, and other devices, may be used with the host computer 102.

Generally, the host computer 102 operates under control of an operating system 108 stored in the memory 106, and interfaces with the user to accept inputs and commands and to present results through a graphical user interface (GUI) module 118A. Although the GUI module 118A is depicted as a separate module, the instructions performing the GUI functions can be resident or distributed in the operating system 108, the computer program 110, or implemented with special purpose memory and processors. The host computer 102 also implements a compiler 112 which allows an application program 110 written in a programming language such as COBOL, C++, FORTRAN, or other language to be translated into processor 104 readable code. After completion, the application 110 accesses and manipulates data stored in the memory 106 of the host computer 102 using the relationships and logic that are generated using the compiler 112. The host computer 102 also comprises an input/output (I/O) port for a personal token 200 (hereinafter alternatively referred to also as a personal key 200). In one embodiment, the I/O port is a USB-compliant interface comprising a host computer USB-compliant interface 130A and a personal token USB-compliant interface 130B (hereinafter referred to collectively as the USB-compliant interface 130.

In one embodiment, instructions implementing the operating system 108, the computer program 110, and the compiler 112 are tangibly embodied in a computer-readable medium, e.g., data storage device 120, which could include one or more fixed or removable data storage devices, such as a zip drive, floppy disc drive 124, hard drive, CD-ROM drive, tape drive, etc. Further, the operating system 108 and the computer program 110 are comprised of instructions which, when read and executed by the computer 102, causes the computer 102 to perform the steps necessary to implement and/or use the present invention. Computer program 110 and/or operating instructions may also be tangibly embodied in memory 106 and/or data communications devices, thereby making a computer program product or article of manufacture according to the invention. As such, the terms "article of manufacture" and "computer program product" as used herein are intended to encompass a computer program accessible from any computer readable device or media.

The host computer 102 may be communicatively coupled to a remote computer or server 134 via communication medium 132 such as a dial-up network, a wide area network (WAN), local area network (LAN), virtual private network (VPN) or the Internet. Program instructions for computer operation, including additional or alternative application programs can be loaded from the remote computer/server 134. In one embodiment, the computer 102 implements an Internet browser, allowing the user to access the world wide web (WWW) and other internet resources.

Those skilled in the art will recognize that many modifications may be made to this configuration without departing from the scope of the present invention. For example, those skilled in the art will recognize that any combination of the above components, or any number of different components, peripherals, and other devices, may be used with the present invention.

FIG. 2 is a block diagram illustrating the components of one embodiment of a personal key 200. The personal key 200 communicates with and obtains power from the host computer 102 through a USB-compliant communication path in the USB-compliant interface 130 which includes the input/output port 130A of the host computer 102 and a matching input/output (I/O) port 130B on the personal key 200. The processor 212 is communicatively coupled to a memory 214, which stores data and instructions to implement the above-described features of the invention. In one embodiment, the memory 214 is a non-volatile random-access memory that can retain factory-supplied data as well as customer-supplied application related data. The processor 212 may also include some internal memory for performing some of these functions.

The processor 212 is optionally communicatively coupled to an input device 218 via an input device communication path 224 and to an output device 222 via an output device communication path 224, both of which are distinct from the USB-compliant interface 130. These separate communication paths 220 and 224 allow the user to view information about processor 212 operations and provide input related to processor 212 operations without allowing a process or other entity with visibility to the USB-compliant interface 130 to eavesdrop or intercede. This permits secure communications between the key processor 212 and the user. In one embodiment of the invention set forth more fully below, the user communicates directly with the processor 212 by physical manipulation of mechanical switches or devices actuatable from the external side of the key (for example, by pressure-sensitive devices such as buttons and mechanical switches). In another embodiment of the invention set forth more fully below, the input device includes a wheel with tactile detents indicating the selection of characters.

The input device and output devices 218, 222 may cooperatively interact with one another to enhance the functionality of the personal key 200. For example, the output device 222 may provide information prompting the user to enter information into the input device 218. For example, the output device 222 may comprise a visual display such as an alphanumeric LED or LCD display (which can display Arabic numbers and or letters) and/or an aural device. The user may be prompted to enter information by a beeping of the aural device, by a flashing pattern of the LED, or by both. The output device 222 may also optionally be used to confirm entry of information by the input device 218. For example, an aural output device may beep when the user enters information into the input device 218 or when the user input is invalid. The input device 218 may take one of many forms, including different combinations of input devices.

Although the input device communication path 220 and the output device communication path 224 are illustrated in FIG. 2 as separate paths, the present invention can be implemented by combining the paths 220 and 224 while still retaining a communication path distinct from the USB-compliant interface 130. For example, the input device 218 and output device 222 may be packaged in a single device and communications with the processor 212 multiplexed over a single communication path.

FIG. 3 is a block diagram of the personal key 200 and host computer 102 as applied to the present invention. Unlike the personal key 200 illustrated in FIG. 2, the personal key 300 illustrated in FIG. 3 comprises a smartcard processor 320. The smartcard processor 300 is a processor which complies with well-known smartcard I/O protocols and smartcard command sets and functions, such as those described by the International Standards Organization (ISO) standard 7816 Part III (defining electronic properties and transmission characteristics), which is hereby incorporated by reference herein.

Physically, the smartcard compliant I/O interface 324 includes a serial I/O line, a reset (RST) line, a clock (CLK) line, a programming voltage (VPP), a power supply voltage (VCC) and a ground. This I/O interface 324 is further described in the publication "Introduction to Smartcards" by Dr. David B. Everett, which was published in 1999 by the Smart Card News Ltd., and is incorporated by reference herein.

As was the case with the personal key 200 and host computer 102 illustrated in FIG. 1, the present invention allows the use of a personal key 300 communicating with the host computer 102 via a USB-compliant interface 130. However, the substitution of the smartcard processor 320 for the ordinary processor 212 depicted in

FIG. 2 has several advantages. First, smartcard processors 212 are relatively inexpensive and readily available. Second, a large number of application programs 110 have been developed for the use of smartcards, including the personal computer/smartcard (PC/SC) interface developed by the MICROSOFT CORPORATION. By providing a smartcard processor (which complies with the smartcard I/O protocols and supports smartcard command sets), this software can be used with a personal key 300 in a USB-compliant form factor. .

The use of the smartcard processor 320 in the personal key 300 is enabled by use of an interface processor 314 communicatively coupled to the smartcard processor 320 via a smartcard-compatible (S/C 7816) interface 324. The interface processor 314 comprises a smartcard reader emulator module (SREM) 316 and a translation module 318. The SREM 316 implements functions that emulate those of a smartcard reader, thus projecting the image of a smartcard reader to the smartcard processor 320. The SREM 316 provides all instructions and commands to the smartcard processor 320 and receives messages and responses from the smartcard processor 320 according to the S/C protocol.

The host computer 102 comprises a virtual smartcard reader module (VSRM) 302. The VSRM comprises a communication module 312, an answer-to-reset module 308, and a smartcard insertion/removal reporting module 306. The communication module 312 packages messages intended for the personal key 300 for transmission via the USB-compliant interface. In one embodiment, messages and commands that are sent to the personal key 300 packaged as:

USB command = USB header + USB cdata (wherein USB cdata is the smartcard compliant command)

and messages and responses from the personal key 300 are packaged as:

USB response = USB header + USB rdata (wherein USB rdata is the smartcard compliant response)

These packaged messages are unpacked by the translation module 318 in the personal key 300. Similarly, messages transmitted by the smartcard processor 320 to the host computer 102 are packaged by the translation module 318 and unpackaged by the communication module 312 before being provided to the operating system 108, the application program interface 260, and the application 110 using the personal key 300 to perform operations.

Just as the SREM 316 emulates the presence of a smartcard reader for the smartcard processor 320, the VSRM 302 emulates the presence of a smartcard reader to the OS 108 in the host computer 102. These functions are accomplished in the bootup module 311, the insert/remove module 306, the answer-to-reset module 308, and the PTS module 310.

As a part of a normal bootup sequence, the host computer's 102 operating system performs a startup sequence to determine which hardware elements are available for use. In prior art smartcard systems, the smartcard reader remains coupled to the host computer 102, whether a smartcard is inserted into the reader or not. Hence, the smartcard reader can respond to startup sequence queries, and the smartcard reader is recognized by the operating system 108 for further operations. However, in the present invention, there is no smartcard reader to answer to the bootup query, and the operating system would ordinarily be unable to operate with a smartcard thereafter. To solve this problem, the present invention comprises a bootup module 311, which responds to messages from the operating system 108 in the same way as a smartcard reader would if it were coupled to the host computer 102.

Similarly, the insert/remove module 306 provides an indication to the operating system 108 that the personal key 300 has been inserted or removed from the

USB-compliant interface 130. This is accomplished by querying the host computer USB-compliant interface port 130A.

When a software application calls 110, via API 260 and the operating system 108 invokes a command that calls for a smartcard related function, the smartcard reader passes a reset command to the smartcard. The smartcard returns an answer-to-reset message which indicates, among other things, the protocol and I/O interface supported by the attached smartcard.

The reset signal is used to start up the program contained in a memory 322 communicatively coupled to or resident within the smartcard processor 320. The ISO standard defines three reset modes, internal reset, active low reset, and synchronous high active reset. Most smartcard processors 320 operate using the active low reset mode. In this mode, the smartcard processor 320 transfers control to the entry address for the program when the reset signal returns to the high voltage level. The synchronous mode of operation is more commonly met with smartcards used for telephonic applications.

The sequence of operations for activating the smartcard processor 320 is defined in order to minimize the possibility of damaging the smartcard processor 320. Of particular importance is avoiding corruption of the non-volatile memory 322 of the smartcard. Most smartcard processors 320 operate using an active low reset mode in which the smartcard processor 320 transfers control to the entry address for the program when the reset signal returns to the high voltage level. The sequence performed by the smartcard processor includes the steps of setting the RST line low, applying VCC to the proper supply voltage, setting the I/O in the receive mode, setting VPP in the idle mode, applying the clock, and taking the RST line high (active low reset).

In prior art smartcard systems, after the reset signal is applied by the smartcard reader, the smartcard processor 320 responds with an answer-to-reset message. For the active low reset mode, the smartcard processor 320 should respond between 400 and 40,000 clock cycles after the rising edge of the reset signal. The answer-to-reset signal is at most 33 characters, and includes 5 fields including an initial character (TS), a format character (TO), interface characters (TAi, TBi, TCi, and TDi), historical characters (T1, T2, . . . , TK), and a check character (TCK). Among other things, the answer-to-reset signal provides an indication of the smartcard protocol(s) which are supported smartcard processor. Typical smartcard protocols include the T=0 protocol (asynchronous half duplex byte transmission) and T=1 (asynchronous half duplex block transmission).

In the embodiment of the present invention shown in FIG. 3, the reset signal is provided by the VSRM 302, packaged by the communication module 312, and sent via the USB-compliant interface 130B to the personal key 300. The message is unwrapped by the translation module 318. Then, the smartcard reader emulation module activates the RST signal path in the smartcard interface 324, thus providing the RST command to the smartcard processor 320. The smartcard processor 320 responds with an answer-to-reset message, sends the message via the serial I/O line of the smartcard interface 324 to the interface processor 314. The message is then packaged by the translation module 318 and transmitted to the host computer 102 via the USB-compliant interface 326. The message is then unpackaged by the communication module 312 and provided to the operating system 108 and ultimately, the application 110 that requested the use of the smartcard.

In another embodiment of the present invention, the personal key 300 does not comprise a smartcard processor 320, but rather a special purpose processor which does not respond to messages and commands in the smartcard I/O protocol (such as that which is illustrated in FIG. 1). The present invention can still be used with existing smartcard applications 110, however, because the VSRM 302 and the interface processor 314 can be used to simulate the presence of a smartcard processor 320. When the smartcard software application 110 desires use of the personal key 300, the VSRM accepts the reset command from the PC/SC modules in the operating system 108, translates the reset message into a functionally equivalent message for the special purpose processor in the personal key 300, and transmits the message to the personal key 300. After the personal key 300 is activated, it sends a message indicating as such to the host computer 102. The VSRM 302, and translates this message to a response that is compatible with the smartcard application 110, namely, an ATR message. Alternatively, the smartcard command to special purpose processor command translation can occur in the emulation processor 314 in the personal key 300.

Returning to the embodiment disclosed in FIG. 3, after the smartcard processor has issued the ATR message, a protocol type selection (PTS) message may be sent to the smartcard processor 320. The PTS message from the OS 108 is received by the PTS module 310 in the VSRM 302, packaged for transmission via the USB-compliant interface 130 to the personal key 300, where it is unpackaged and provided to the smartcard processor 320. The smartcard provides a response consistent with the ISO standards to the emulation module 316. The response is packaged, and transmitted over the USB-compliant interface 130 to the host computer 102, where it is unpackaged by the communication module 312 and provided to the operating system.

FIGs. 4A-4D are flow charts presenting exemplary method steps used to practice one embodiment of the present invention. When the host computer 102 is booted up, the virtual smartcard reader 302 accepts 402 a bootup query from the host computer's operating system 108. Although a smartcard reader is not communicatively coupled to the host computer 130 the virtual smartcard reader 302 emulates the existence of a smartcard reader and provides an indication that a smartcard reader is available to the OS 108. Consequently, when the bootup procedures are completed, a smartcard reader will be registered as an available device to smartcard applications 110.

When the host computer is booted up, a personal key 300 may or may not be communicatively coupled to the USB-compliant interface 130. When a personal key 300 is not attached, the VSRM 302 provides 404 the same indication to the operating system 108 as would be supplied by a smartcard reader without an inserted smartcard. This is accomplished by receiving 406 an indication that the personal key has been communicatively coupled to the USB-compliant interface; and providing an indication to the host computer operating system. Since the VSRM is emulating the functions of a smartcard, the indication is provided 408 to the host computer operating system (or equivalently, the personal computer/smartcard (PC/SC) interface modules therein) is that of an insert event.

If desired and the smartcard processor 320 supports multiple protocols, a protocol type selection (PTS) command may be issued by the operating system 108. The VSRM 302 receives 410 the PTS command, packages the command for transmission to the personal key 300 via the USB-compliant interface 130. The wrapped PTS command is then transmitted over the USB-compliant interface 130 and received by the personal key 300. The PTS command is unwrapped by the translate module 318 in the interface processor 314 and provided to the smartcard processor 320 via the smartcard-compliant interface 324. The smartcard processor computes the appropriate response, sends the response to the interface processor 314, where the response is packaged by the translate module 318 for transmission to the host computer 102 via the USB-compliant interface 130. The communication module 312 unpackages the response, and the PTS module 310 formats the response, if necessary, to be consistent with a PTS response received from a smartcard reader. The formatted response is then provided 412 to the OS 108.

FIG. 4B is a flow chart describing exemplary method steps used to provide commands and/or data from the OS 108 to the smartcard processor 320 and from the smartcard processor 320 to the OS 108. A message, which may comprise a smartcard reader command belonging to a smartcard reader command set is accepted 414 from a host computer operating system 108 in the virtual smartcard reader module (VSRM) 302. The message is packaged 416 for transmission via the USB-compliant interface 130 according to a first message transfer protocol.

The packaged message is then transmitted 418 to the communicatively coupled personal key 300 via the USB-compliant interface 130. The packaged message is received 420 and unpackaged 422 in the personal key 300. If the smartcard reader command requires additional processing before being forwarded to the smartcard processor 320, the smartcard reader command is translated 424 into a smartcard command within the personal key 300 before being provided 426 to the smartcard processor 320.

The smartcard processor 320 then performs the indicated operation, and a response is accepted 428 from the smartcard processor 320. If the smartcard response requires further processing by a smartcard reader, the smartcard response is translated 430 into a smartcard reader response. The smartcard reader response is then packaged 432 and transmitted 434 to the host computer 102 via the USB-compliant interface 130. The host computer 102 receives 436 and unpackages 438 the message and provides 440 the response to the smartcard software application 110 that issued the command.

Next, when the personal key 300 is removed, the VSRM 302 reports 444 an indication to the OS 108 that the "virtual smartcard" (the personal key 300) has been removed. The provided indication is the same as that which would be provided by a smartcard reader when a smartcard is removed. The indication can be obtained, for example by receiving 442 an indication from a USB driver or other device indicating the removal of a USB device.

In summary, Tables I and II provides an summary of the communication protocol for an OS 108 command from the host computer 102 to the smartcard processor 320 in the personal key (Table I), and for a smartcard processor 320 response to the operating system 108.

Step	Description
1	Smartcard reader command issued from OS 108 is passed to VSRM 302
2	VSRM 302 adds a USB header, and creates a USB command
3	VSRM's 302 communication module 312 sends the USB command to the personal key 300
4	The translation module 318 strips off the USB header and recovers the smartcard command
5	The smartcard command is sent to the smartcard processor 320
6	The smartcard processor 320 executes the function requested by the smartcard command

Table I

Step	Description
1	Smartcard processor 320 generates a smartcard response
2	The smartcard response is sent from the smartcard processor 320 to the translation module 318
3	The translation module 318 adds a USB header to create a USB response
4	The USB response is transmitted to the VSRM 302
5	The communication module 312 strips off the USB header and recovers the smartcard response
6	The smartcard response is transmitted to the OS 108

Table II

Tables III and IV provides a summary of the communication protocol for a request from an application program 110 to the smartcard processor 320 and for a request from an application program 110 to the smartcard processor 320.

Step	*Description*
1	Smartcard processor 320 command from the application program 110 is sent to the OS 108 via an API 260
2	The smartcard processor 320 command is sent from the OS 108 to the VSRM 302
3	The VSRM 302 adds a USB header to the smartcard processor 320 command to create a USB-compatible command
4	The VSRM's comm module 312 sends the USB-compliant command to the personal key 300
5	Translation module 318 strips off the USB header and recovers the smartcard processor command
6	The smartcard processor command is transmitted to the smartcard processor 320
7	The smartcard processor 320 performs the function indicated by the smartcard processor command

Table III

Step	Description
1	The smartcard processor 320 generates a response to the smartcard processor command
2	The response is provided to the translation module 318
3	The translation module adds a USB header to create a USB-compatible smartcard processor response
4	The USB-compatible smartcard processor response is sent to the VSRM 302
5	The communication module 312 strips off the USB header to recover the smartcard processor response
6	The smartcard processor response is provided to the application 110 via the OS 108 and the API 260

Table IV

Conclusion

This concludes the description of the preferred embodiments of the present invention. In summary, the present invention describes a personal key comprising a USB-compliant interface releaseably coupleable to a host processing device operating under command of an operating system; a smartcard processor having a smartcard processor-compliant interface for communicating according to a smartcard input and output protocol; and an interface processor, communicatively coupled to the USB-compliant interface and to the smartcard processor-compliant interface, the interface processor implementing a translation module for interpreting USB-compliant messages into smartcard processor-compliant messages and for interpreting smartcard processor-compliant messages into USB-compliant messages. In another embodiment, the invention is described by a method comprising the steps of accepting a message comprising a smartcard reader command selected from a smartcard reader command set from a host computer operating system in a virtual smartcard reader; packaging the message for transmission via a USB-compliant interface according to a first message transfer protocol; transmitting the packaged message to a personal key communicatively coupled to the USB-compliant interface; receiving the packaged message in the personal key; unpackaging the message in the personal key to recover the smartcard reader command; translating the smartcard reader command into a smartcard command within the personal key; and providing the smartcard command to the smartcard processor.

The foregoing description of the preferred embodiment of the invention has been presented for the purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed. Many modifications and variations are possible in light of the above teaching. It is intended that the scope of the invention be limited not by this detailed description, but rather by the claims appended hereto. The above specification, examples and data provide a complete description of the manufacture and use of the composition of the invention. Since many embodiments of the invention can be made without departing from the spirit and scope of the invention, the invention resides in the claims hereinafter appended.

WHAT IS CLAIMED IS:

1. A compact personal token (300), comprising:

a USB-compliant interface (130B) releaseably coupleable to a host processing device (102) operating under command of an operating system (108);

a smartcard processor (320) having a smartcard processor-compliant interface (324) for communicating according to a smartcard input and output protocol;

an input device (218) communicatively coupled to the smartcard processor for providing secure input to the processor;

an interface processor (314), communicatively coupled to the USB-compliant interface (130B) and to smartcard processor-compliant interface (324) the interface processor (314) implementing a translation module (318) for interpreting USB-compliant messages into smartcard processor-compliant messages and for interpreting smartcard processor-compliant messages into USB-compliant messages.

2. The apparatus of claim 1, wherein the interface processor (314) emulates a smartcard reader to the smartcard processor (320).

3. The apparatus of claim 1, wherein:

the host processing device (102) comprises a virtual smartcard reader in communication with the operating system, the virtual smartcard reader for emulating a smartcard reader communicatively coupled to the host processing device (102) and including a communication module (312) for packaging messages for transmission to the personal token (300) via the USB compliant interface (130) according to a first protocol and for unpackaging messages received from the personal token (300) via the USB-compliant interface according to the first protocol; and

the interface processor translation module (318) unpackages messages from the host processing device (102) according to the first protocol and packages messages destined for the host processing device (102) according to the first protocol.

4. The apparatus of claim 3, wherein the virtual smartcard reader further comprises a bootup module (311) for responding to an operating system bootup procedure with an indication that a smartcard reader is communicatively coupled to the host processor.

5. The apparatus of claim 3, wherein the virtual smartcard reader further comprises an answer-to-reset (ATR) module (308) for providing an ATR message to the operating system (108) in response to a reset message.

6. The apparatus of claim 3, wherein the virtual smartcard reader further comprises a reporting module for receiving and reporting the insertion of the personal token in a USB-compliant port communicatively coupled to the host processor (102) and the removal of the personal token as a removal of a smartcard from a smartcard reader.

7. The apparatus of claim 3, wherein the virtual smartcard reader further comprises a protocol selection module for receiving a protocol type selection (PTS) command from the operating system and providing a PTS response message to the operating system (108).

8. A method of communicating between a smartcard processor (320) in a personal key (300) communicatively coupled to a host computer (102) via a USB-compliant interface (130), comprising the steps of:

accepting a message comprising a smartcard reader command selected from a smartcard reader command set from a host computer operating system (108) in a virtual smartcard reader;

packaging the message for transmission via a USB-compliant interface (130) according to a first message transfer protocol;

transmitting the packaged message to a personal key (300) communicatively coupled to the USB-compliant interface (130);

receiving the packaged message in the personal key (300);

unpackaging the message in the personal key (300) to recover the smartcard reader command;

translating the smartcard reader command into a smartcard command within the personal key (300); and

providing the smartcard command to the smartcard processor (320);

accepting a user input to the smartcard processor (320) via an input device (218) communicatively coupled to the smartcard processor (320) via an input communication device communication path distinct from the USB-compliant interface (130);

accepting a smartcard response from the smartcard processor (320);

translating the smartcard response into a smartcard reader response;

packaging the smartcard reader response for transmission to the host processor (102) via the USB-compliant interface (130);

transmitting the packaged message from the personal key (300) to the host processor (102);

receiving the packaged message in the host computer (102);

unpackaging the smartcard reader response; and

providing the smartcard reader response to the host processor operating system (108).

9. The method of claim 8, further comprising the steps of:

accepting a startup query from the host computer operating system (108) in the virtual smartcard reader; and

providing an indication that a smartcard reader is communicatively coupled to the host computer to the host computer operating system (108).

10. The method of claim 9, further comprising the steps of:

receiving an indication that the personal key (300) has been communicatively coupled to the USB-compliant interface (130);

reporting the indication that the personal key (300) is communicatively coupled to the USB-compliant interface (130) to the host processor operating system (108) as the insertion of a smartcard;

receiving an indication that the personal key (300) has been communicatively decoupled from the USB-compliant interface (130); and

reporting the indication that the personal key has been communicatively decoupled from the USB-compliant interface (130) to the host processor operating system (108) as the removal of the smartcard.

11. The method of claim 8, further comprising the steps of:

receiving a protocol type selection (PTS) command from the host computer operating system (108); and

providing a PTS response message to the operating system (108).

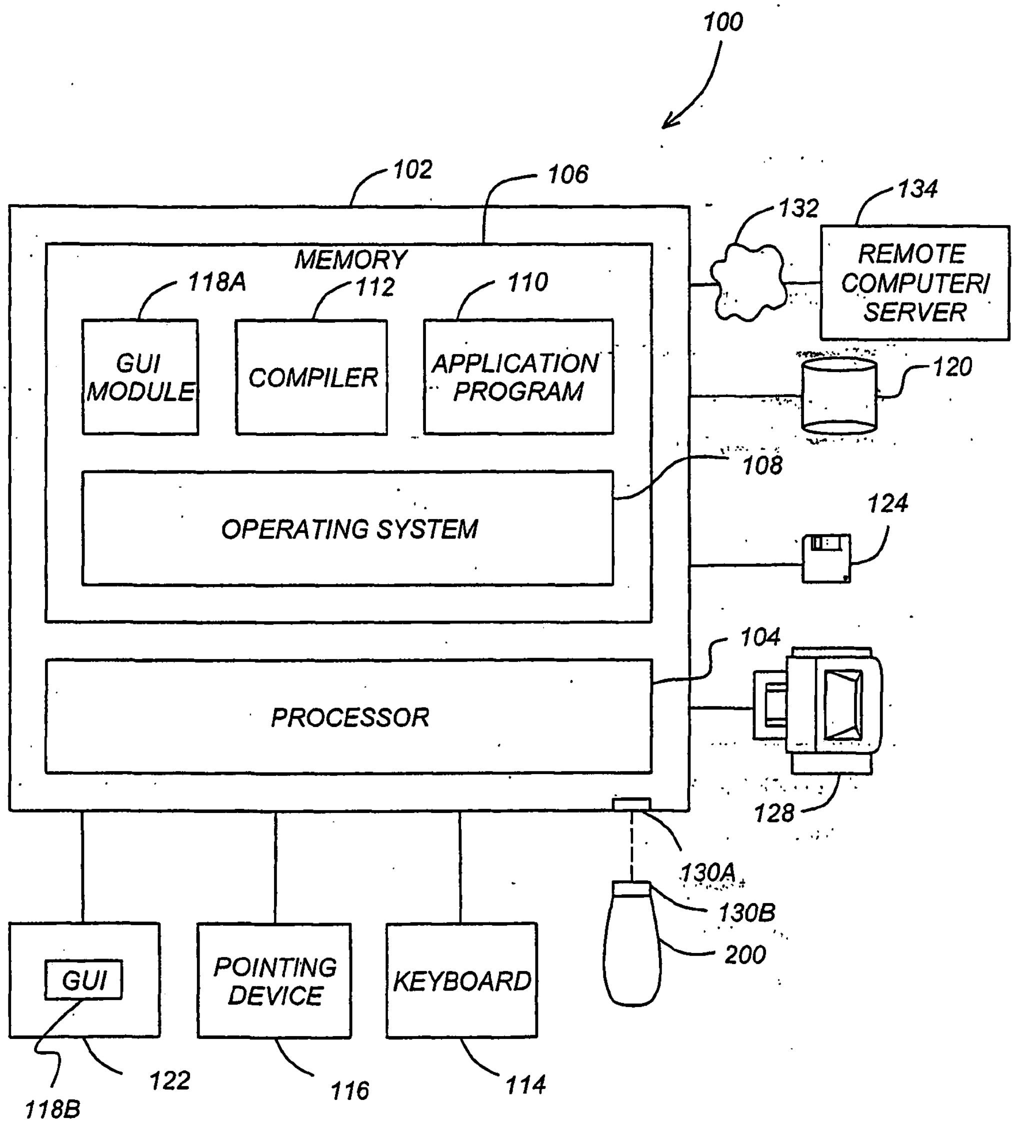

100
102
106
MEMORY
118A
112
110
GUI MODULE
COMPILER
APPLICATION PROGRAM
OPERATING SYSTEM
108
PROCESSOR
104
132
134
REMOTE COMPUTER/ SERVER
120
124
128
130A
130B
200
GUI
POINTING DEVICE
KEYBOARD
118B
122
116
114

FIG. 1

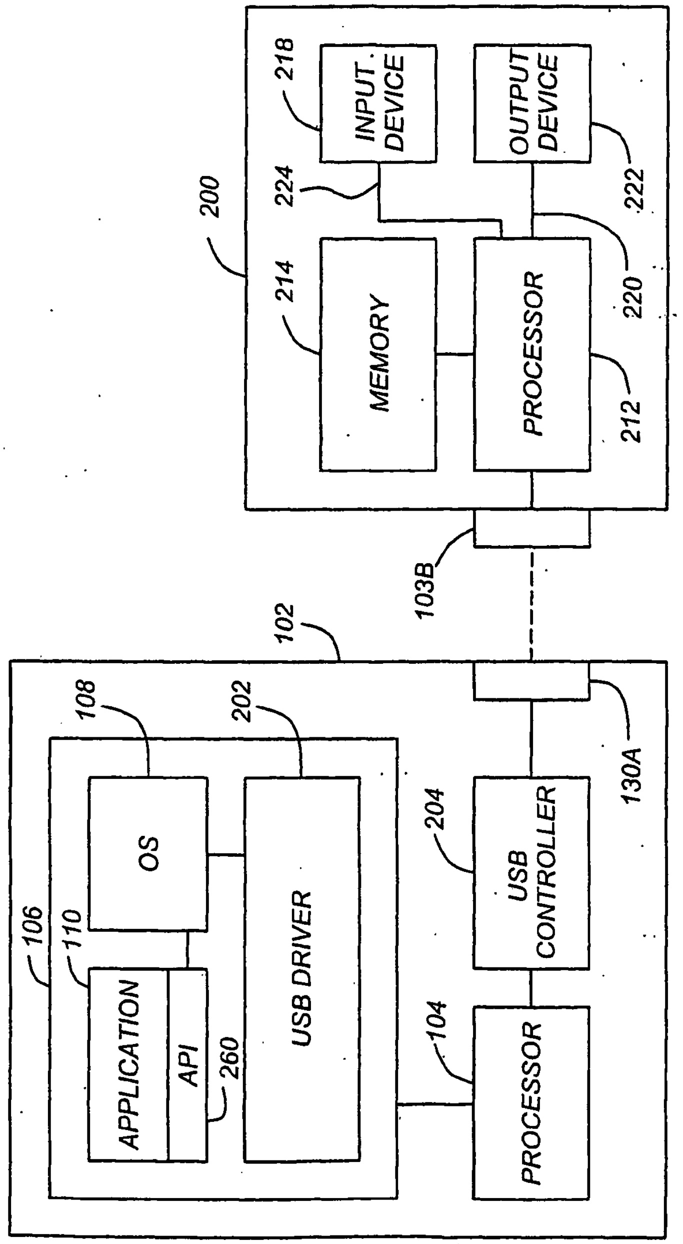
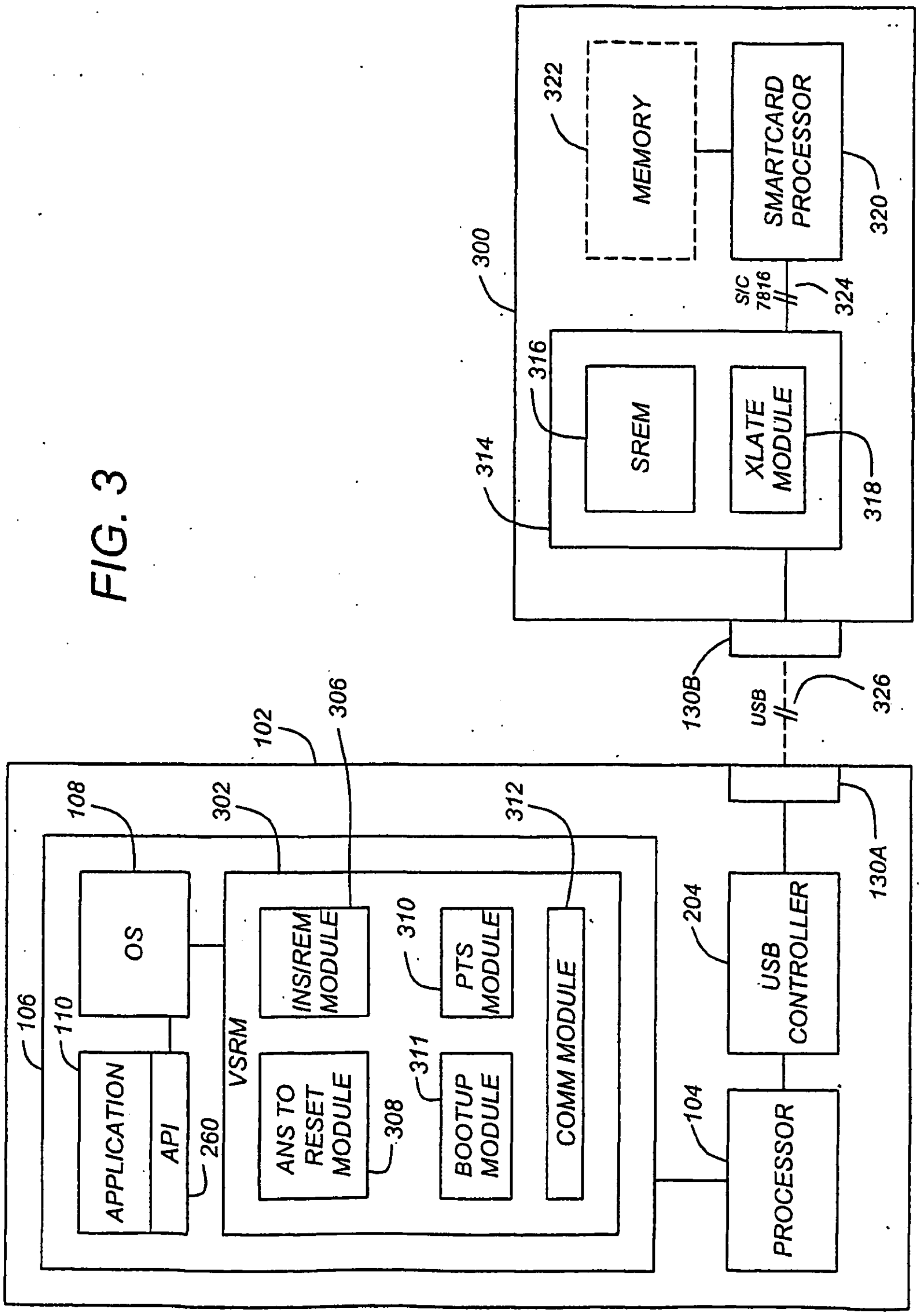

200
218
INPUT DEVICE
OUTPUT DEVICE
224
222
214
MEMORY
PROCESSOR
220
212
103B
102
108
202
OS
USB DRIVER
106
110
APPLICATION
API
260
204
USB CONTROLLER
130A
104
PROCESSOR

FIG. 2

FIG. 3


300
322
MEMORY
SMARTCARD PROCESSOR
320
S/C 7816
324
314
316
SREM
XLATE MODULE
318
130B
USB
326
102
306
108
302
312
106
110
OS
APPLICATION
API
260
VSRM
INS/REM MODULE
310
PTS MODULE
ANS TO RESET MODULE
308
311
BOOTUP MODULE
COMM MODULE
104
204
USB CONTROLLER
PROCESSOR
130A

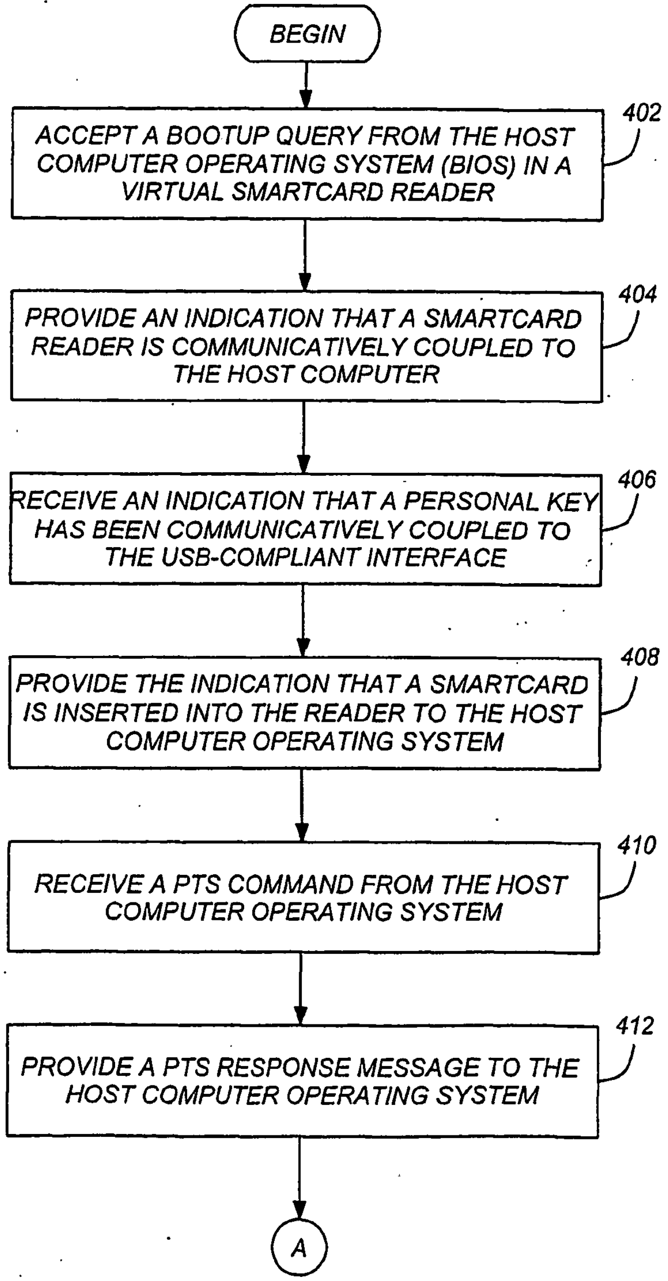

BEGIN
ACCEPT A BOOTUP QUERY FROM THE HOST COMPUTER OPERATING SYSTEM (BIOS) IN A VIRTUAL SMARTCARD READER
402
PROVIDE AN INDICATION THAT A SMARTCARD READER IS COMMUNICATIVELY COUPLED TO THE HOST COMPUTER
404
RECEIVE AN INDICATION THAT A PERSONAL KEY HAS BEEN COMMUNICATIVELY COUPLED TO THE USB-COMPLIANT INTERFACE
406
PROVIDE THE INDICATION THAT A SMARTCARD IS INSERTED INTO THE READER TO THE HOST COMPUTER OPERATING SYSTEM
408
RECEIVE A PTS COMMAND FROM THE HOST COMPUTER OPERATING SYSTEM
410
PROVIDE A PTS RESPONSE MESSAGE TO THE HOST COMPUTER OPERATING SYSTEM
412
A

FIG. 4A

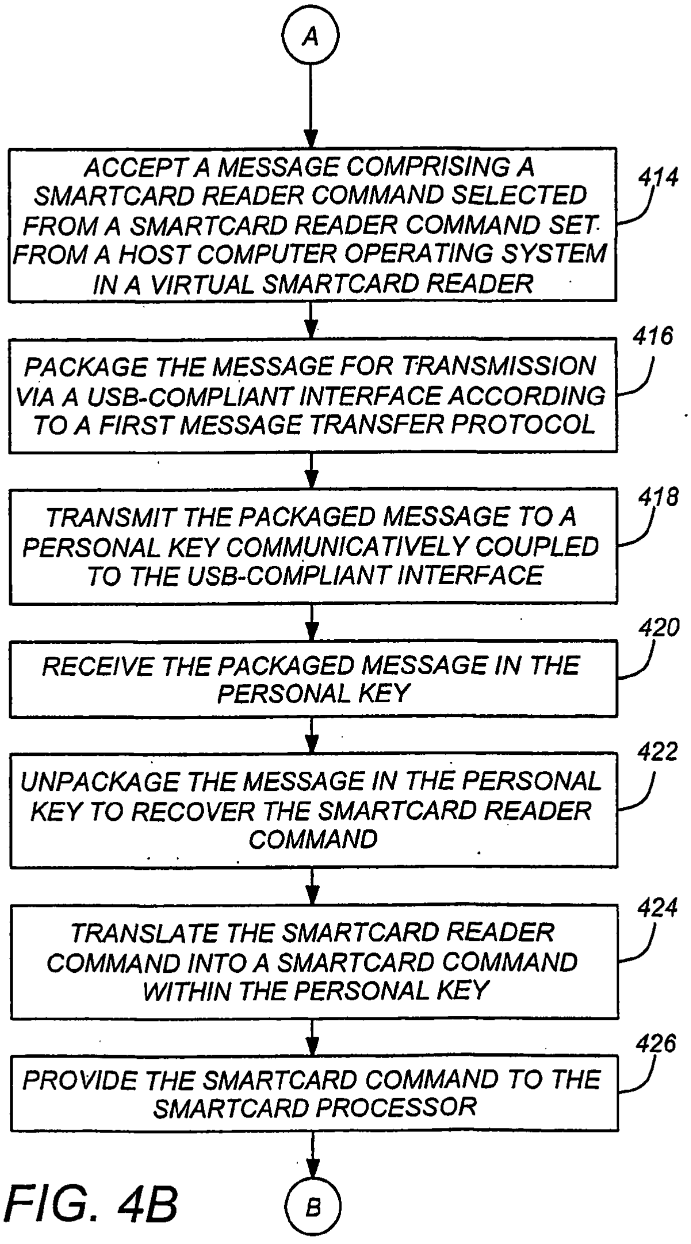

A
ACCEPT A MESSAGE COMPRISING A SMARTCARD READER COMMAND SELECTED FROM A SMARTCARD READER COMMAND SET FROM A HOST COMPUTER OPERATING SYSTEM IN A VIRTUAL SMARTCARD READER
414
PACKAGE THE MESSAGE FOR TRANSMISSION VIA A USB-COMPLIANT INTERFACE ACCORDING TO A FIRST MESSAGE TRANSFER PROTOCOL
416
TRANSMIT THE PACKAGED MESSAGE TO A PERSONAL KEY COMMUNICATIVELY COUPLED TO THE USB-COMPLIANT INTERFACE
418
RECEIVE THE PACKAGED MESSAGE IN THE PERSONAL KEY
420
UNPACKAGE THE MESSAGE IN THE PERSONAL KEY TO RECOVER THE SMARTCARD READER COMMAND
422
TRANSLATE THE SMARTCARD READER COMMAND INTO A SMARTCARD COMMAND WITHIN THE PERSONAL KEY
424
PROVIDE THE SMARTCARD COMMAND TO THE SMARTCARD PROCESSOR
426
B

FIG. 4B

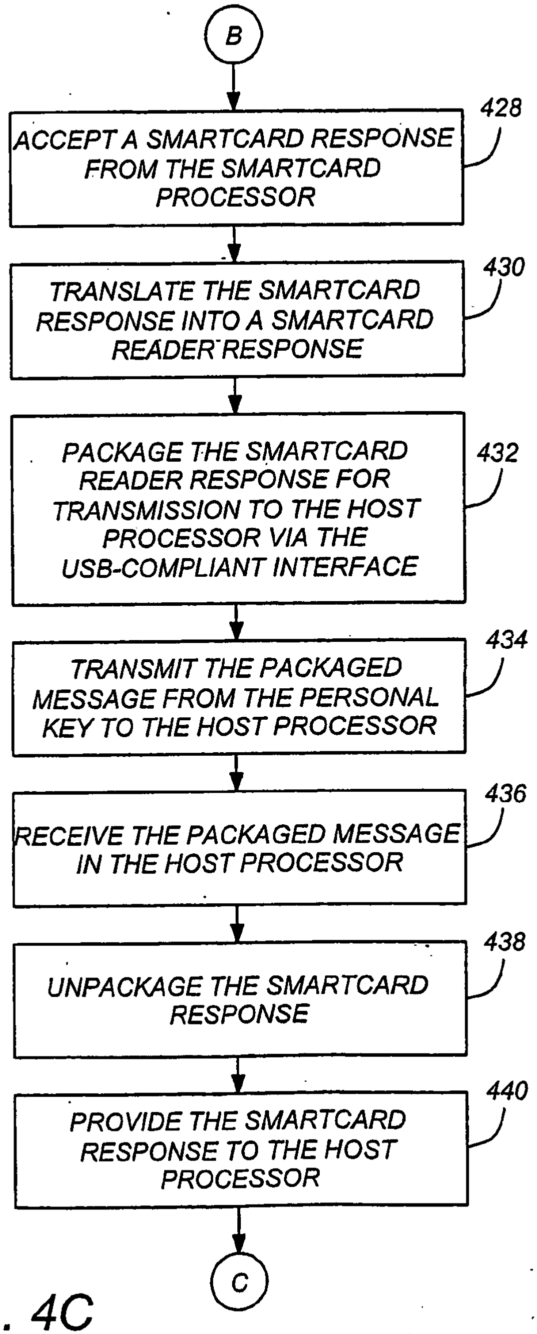

B
ACCEPT A SMARTCARD RESPONSE FROM THE SMARTCARD PROCESSOR
428
TRANSLATE THE SMARTCARD RESPONSE INTO A SMARTCARD READER RESPONSE
430
PACKAGE THE SMARTCARD READER RESPONSE FOR TRANSMISSION TO THE HOST PROCESSOR VIA THE USB-COMPLIANT INTERFACE
432
TRANSMIT THE PACKAGED MESSAGE FROM THE PERSONAL KEY TO THE HOST PROCESSOR
434
RECEIVE THE PACKAGED MESSAGE IN THE HOST PROCESSOR
436
UNPACKAGE THE SMARTCARD RESPONSE
438
PROVIDE THE SMARTCARD RESPONSE TO THE HOST PROCESSOR
440
C

FIG. 4C

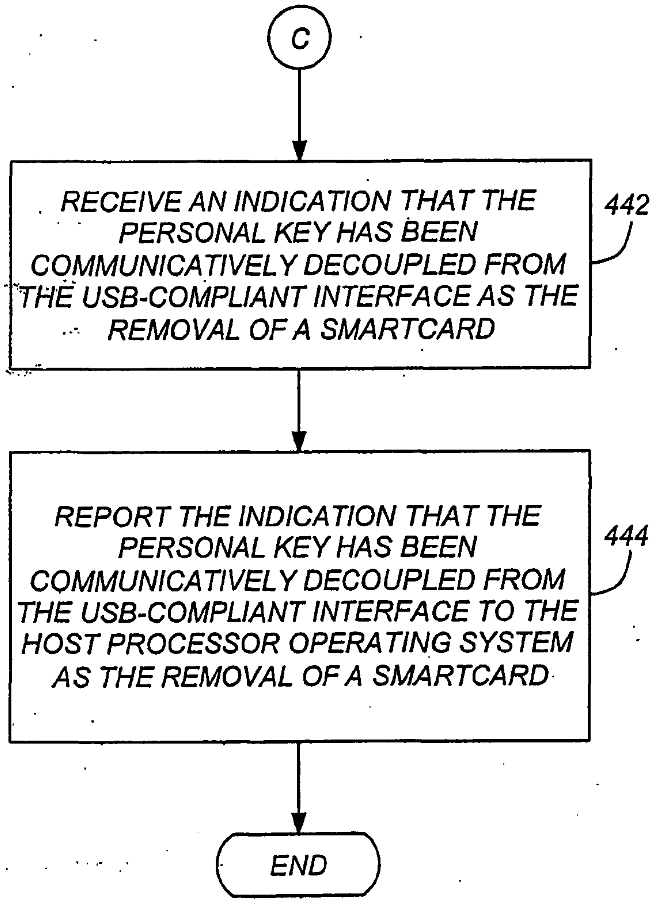

C
RECEIVE AN INDICATION THAT THE PERSONAL KEY HAS BEEN COMMUNICATIVELY DECOUPLED FROM THE USB-COMPLIANT INTERFACE AS THE REMOVAL OF A SMARTCARD
442
REPORT THE INDICATION THAT THE PERSONAL KEY HAS BEEN COMMUNICATIVELY DECOUPLED FROM THE USB-COMPLIANT INTERFACE TO THE HOST PROCESSOR OPERATING SYSTEM AS THE REMOVAL OF A SMARTCARD
444
END

FIG. 4D

UNITED STATES PATENT AND TRADEMARK OFFICE

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

Bib Data Sheet

CONFIRMATION NO. 2050

SERIAL NUMBER 10/990,296	FILING DATE 11/16/2004 RULE	CLASS 235	GROUP ART UNIT 2876	ATTORNEY DOCKET NO. Ryan C-4

APPLICANTS

Dennis J. Ryan, Chandler, AZ;

David Finn, Mayo, IRELAND;
Patrick R. Comiskey, University Heights, OH;Norbert Knapich, Rosshaupten, GERMANY;

** CONTINUING DATA *************************
This appln claims benefit of 60/520,698 11/17/2003
and claims benefit of 60/562,204 04/14/2004
and claims benefit of 60/602,595 08/18/2004

** FOREIGN APPLICATIONS ********************

IF REQUIRED, FOREIGN FILING LICENSE GRANTED ** 12/16/2004

** SMALL ENTITY **

Foreign Priority claimed □ yes ☑ no 35 USC 119 (a-d) conditions met □ yes ☑ no □ Met after Allowance Verified and Acknowledged ______ Examiner's Signature ______ Initials	STATE OR COUNTRY AZ	SHEETS DRAWING 4	TOTAL CLAIMS 52	INDEPENDENT CLAIMS 3

ADDRESS
37053
D.A. STAUFFER PATENT SERVICES LLC
1006 MONTFORD ROAD
CLEVLAND HTS. , OH
44121-2016

TITLE
Multi-interface compact personal token apparatus and methods of use

FILING FEE	FEES: Authority has been given in Paper	□ All Fees □ 1.16 Fees (Filing) □ 1.17 Fees (Processing Ext. of time)

Index of Claims

Application/Control No. 10/990,296	**Applicant(s)/Patent under Reexamination** RYAN ET AL.
Examiner Uyen-Chau N. Le	**Art Unit** 2876

√	Rejected	–	(Through numeral) Cancelled	N	Non-Elected	A	Appeal
=	Allowed	+	Restricted	I	Interference	O	Objected

Claim		Date								
Final	Original	7/7/05								
	1	√								
	2	│								
	3	│								
	4	│								
	5	│								
	6	│								
	7	│								
	8	│								
	9	│								
	10	│								
	11	│								
	12	│								
	13	│								
	14	│								
	15	│								
	16	│								
	17	│								
	18	│								
	19	│								
	20	│								
	21	│								
	22	│								
	23	│								
	24	│								
	25	│								
	26	│								
	27	│								
	28	│								
	29	│								
	30	│								
	31	│								
	32	│								
	33	│								
	34	│								
	35	│								
	36	│								
	37	│								
	38	│								
	39	│								
	40	│								
	41	│								
	42	│								
	43	│								
	44	│								
	45	│								
	46	│								
	47	│								
	48	│								
	49	│								
	50	√								
	51	√								
	52	√								
	53									
	54									
	55									
	56									
	57									
	58									
	59									
	60									
	61									
	62									
	63									
	64									
	65									
	66									
	67									
	68									
	69									
	70									
	71									
	72									
	73									
	74									
	75									
	76									
	77									
	78									
	79									
	80									
	81									
	82									
	83									
	84									
	85									
	86									
	87									
	88									
	89									
	90									
	91									
	92									
	93									
	94									
	95									
	96									
	97									
	98									
	99									
	100									
	101									
	102									
	103									
	104									
	105									
	106									
	107									
	108									
	109									
	110									
	111									
	112									
	113									
	114									
	115									
	116									
	117									
	118									
	119									
	120									
	121									
	122									
	123									
	124									
	125									
	126									
	127									
	128									
	129									
	130									
	131									
	132									
	133									
	134									
	135									
	136									
	137									
	138									
	139									
	140									
	141									
	142									
	143									
	144									
	145									
	146									
	147									
	148									
	149									
	150									

U.S. Patent and Trademark Office

Part of Paper No. 7605

Search Notes	Application/Control No. 10/990,296	Applicant(s)/Patent under Reexamination RYAN ET AL.	
	Examiner Uyen-Chau N. Le	**Art Unit** 2876	

SEARCHED

Class	Subclass	Date	Examiner
235	380		
	375		
	492		
705	41		
	44		
713	172		
	200		
	201	7/7/2005	UCL

INTERFERENCE SEARCHED

Class	Subclass	Date	Examiner

SEARCH NOTES (INCLUDING SEARCH STRATEGY)

	DATE	EXMR
EAST (ATTACHED)	7/7/2005	UCL
PLUS SEARCH	7/5/2005	UCL

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	162	personal near10 (token fob key) same usb	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/07/07 17:31
L2	138	1 and @ad<="20031117"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/07/07 17:31
L3	50	("6439464" "6128673" "6343364" "6883715" "6131125" "6370603" "6567273" "6628325" "6694399" "6750902" "6752321" "6769622" "6772956" "6843423" "6910638" "6098171" "6151647" "6168077" "6199128" "6581122" "6634565" "6738259" "6763399" "6779059" "6801956" "6817534" "6883718" "6598032" "6748541" "6779734" "6874680" "6543690" "6783078" "6793144" "6913196" "6914695" "6205505" "5875313" "5937175" "5953511" "5968142" "6058441" "6125409" "6286063" "6385677" "6625472" "6629181" "6658516" "6731751" "6738856").pn.	US-PGPUB; USPAT	OR	ON	2005/07/07 17:31
L4	47	("6745267" "6061746" "6061746" "5841471" "5890016" "5930496" "5933656" "5951667" "5963726" "5970220" "5987106" "6073188" "6085156" "6105143" "6178458" "6192420" "6199122" "6206480" "6217389" "6223134" "6217389" "6223134" "6243778" "6246578" "6251014" "6270415" "6289405" "6292863" "6301104" "6343260" "6356968" "6405145" "6418392" "6424525" "6443839" "6449662" "6480801" "6524137" "6525932" "6546441" "6557754" "6581123" "6607139" "6614708" "6651184" "6654841" "6676420" "6712698" "6722985" "6736678").pn.	US-PGPUB; USPAT	OR	ON	2005/07/07 17:31
L5	204	usb adj (token fob key)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/07/07 17:31

L6	148	5 and @ad<="20031117"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/07/07 17:31

IFW

PTO/SB/21 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	10/990,296
Filing Date	Nov. 16, 2004
First Named Inventor	Dennis J. Ryan
Art Unit	2876
Examiner Name	Uyen Chau N. Lee
Attorney Docket Number	Ryan C-4
Total Number of Pages in This Submission	6

ENCLOSURES *(Check all that apply)*

☑ Fee Transmittal Form
- ☑ Fee Attached

☐ Amendment/Reply
- ☐ After Final
- ☐ Affidavits/declaration(s)

☐ Extension of Time Request

☐ Express Abandonment Request

☑ Information Disclosure Statement

☐ Certified Copy of Priority Document(s)

☐ Reply to Missing Parts/ Incomplete Application
- ☐ Reply to Missing Parts under 37 CFR 1.52 or 1.53

☐ Drawing(s)

☐ Licensing-related Papers

☐ Petition

☐ Petition to Convert to a Provisional Application

☐ Power of Attorney, Revocation Change of Correspondence Address

☐ Terminal Disclaimer

☐ Request for Refund

☑ CD, Number of CD(s) 1
- ☐ Landscape Table on CD

☐ After Allowance Communication to TC

☐ Appeal Communication to Board of Appeals and Interferences

☐ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**

☐ Proprietary Information

☐ Status Letter

☒ Other Enclosure(s) (please Identify below):

RECEIPT POSTCARD

Remarks

DUE TO THE LARGE NUMBER OF PAGES TO BE SUBMITTED FOR THE NON-USP REFERENCE DOCUMENTS IN THE IDS, THESE DOCUMENTS ARE SUBMITTED IN ACROBAT READER (PDF) FORMAT IN THE ENCLOSED CD.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	D.A. STAUFFER PATENT SERVICES LLC		
Signature	DAStauffer		
Printed name	DWIGHT A. STAUFFER		
Date	9/9/05	Reg. No.	47,963

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature	DAStauffer		
Typed or printed name	DWIGHT A. STAUFFER	Date	9/9/05

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

PTO/SB/17 (12-04v2)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Effective on 12/08/2004.
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL
For FY 2005

☑ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) 180

Complete if Known	
Application Number	10/990,296
Filing Date	Nov. 16, 2004
First Named Inventor	Dennis J. Ryan
Examiner Name	Uyen Chau N. Lee
Art Unit	2876
Attorney Docket No.	Ryan C-4

METHOD OF PAYMENT (check all that apply)

□ Check ☑ Credit Card □ Money Order □ None □ Other (please identify): ____________

□ Deposit Account Deposit Account Number: ____________ Deposit Account Name: ____________

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☑ Charge fee(s) indicated below □ Charge fee(s) indicated below, **except for the filing fee**

☑ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☑ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

	FILING FEES		SEARCH FEES		EXAMINATION FEES		
Application Type	Fee ($)	Small Entity Fee ($)	Fee ($)	Small Entity Fee ($)	Fee ($)	Small Entity Fee ($)	Fees Paid ($)
Utility	300	150	500	250	200	100	________
Design	200	100	100	50	130	65	________
Plant	200	100	300	150	160	80	________
Reissue	300	150	500	250	600	300	________
Provisional	200	100	0	0	0	0	________

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	50	25
Each independent claim over 3 (including Reissues)	200	100
Multiple dependent claims	360	180

Total Claims **Extra Claims** **Fee ($)** **Fee Paid ($)**
________ - 20 or HP = ________ x ________ = ________
HP = highest number of total claims paid for, if greater than 20.

Multiple Dependent Claims
Fee ($) **Fee Paid ($)**
________ ________

Indep. Claims **Extra Claims** **Fee ($)** **Fee Paid ($)**
________ - 3 or HP = ________ x ________ = ________
HP = highest number of independent claims paid for, if greater than 3.

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets **Extra Sheets** **Number of each additional 50 or fraction thereof** **Fee ($)** **Fee Paid ($)**
________ - 100 = ________ / 50 = ________ (round **up** to a whole number) x ________ = ________

4. OTHER FEE(S) **Fees Paid ($)**

Non-English Specification, $130 fee (no small entity discount) ________

Other (e.g., late filing surcharge): Submission of IDS after first Office Action 180

SUBMITTED BY

Signature	DAStauffer	Registration No. (Attorney/Agent) 47,963	Telephone 216-381-6599
Name (Print/Type)	DWIGHT A. STAUFFER		Date 9/9/05

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

09/14/2005 GWORDOF1 00000001 10990296

01 FC:1806 180.00 OP

substitute forms PTO/SB/08a & PTO/SB/08b		Application Number	**10/990,296**
		Filing Date	**November 16, 2004**
INFORMATION DISCLOSURE STATEMENT BY APPLICANT		First Named Inventor	Dennis J. Ryan
		Art Unit	2876
		Examiner Name	Uyen Chau N. Lee
Sheet 1 OF 3		Practitioner Docket No.	Ryan C-4

U.S. PATENT DOCUMENTS

Exam. Initials	Cite No.	Document Number No. -Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Relevant Pages, Columns, Lines
	A	US-3,941,489	03-22-1974	Bryan	
	B	US-4,367,965	01-11-1983	Speitel et al.	
	C	US-5,761,648	06-02-1998	Golden et al.	
	D	US-6,067,235	05-23-2000	Finn et al.	
	E	US 6,085,320	07-04-2000	Kaliski, Jr.	
	F	US 6,148,354	11-14-2000	Ban et al.	
	G	US 6,168,077	01-02-2001	Gray et al.	
	H	US 6,189,098	02-13-2001	Kaliski, Jr.	
	I	US 6,240,184	05-29-2001	Huynh et al.	
	J	US 6,283,658	09-04-2001	Estevez et al.	
	K	US 6,370,603	04-09-2002	Silverman et al.	
	L	US 6,385,677	05-07-2002	Yao	
	M	US 6,505,773	01-14-2003	Palmer et al.	
	N	US 6,543,690	04-08-2003	Leydier et al.	
	O	US 6,567,273	05-20-2003	Liu et al.	
	P	US 6,658,516	12-02-2003	Yao	
	Q	US 6,694,399	02-17-2004	Leydier et al.	
	R	US 6,724,680	04-20-2004	Ng et al.	
	S	US 6,748,541	06-08-2004	Margalit et al.	
	T	US 6,752,321	06-22-2004	Leaming	
	U	US 6,763,399	07-13-2004	Margalit et al.	
	V	US 6,772,956	08-10-2004	Leaming	
	W	US 6,798,169	09-28-2004	Stratmann et al.	
	X	US 6,801,956	10-05-2004	Feuser et al.	
	Y	US 6,848,045	01-25-2005	Long et al.	
	Z	US 6,876,420	04-05-2005	Hong et al.	
	AA	US 6,879,597	04-12-2005	Tordera et al.	
	BB	US 2001 0043702	11-22-2001	Elteto et al.	
	CC	US 2001 0054148	12-20-2001	Hoornaert	
	DD	US 2002 0011516	01-31-2002	Lee	
	EE	US 2003 0000267	01-02-2003	Jacob et al.	
	FF	US 2003 0028797	02-06-2003	Long et al.	
	GG	US 2003 0087601	05-08-2003	Agam et al.	
	HH	US 2003 0102380	06-05-2003	Spencer	
	II	US 2003 0236821	12-25-2003	Jiau	

substitute forms PTO/SB/08a & PTO/SB/08b	Application Number	**10/990,296**
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	**November 16, 2004**
	First Named Inventor	Dennis J. Ryan
	Art Unit	2876
	Examiner Name	Uyen Chau N. Lee
Sheet 2 OF 3	Practitioner Docket No.	Ryan C-4

FOREIGN PATENT DOCUMENTS

Exam. Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Doc.	Relevant Pages, Columns, Lines	T
	f1	DE19631050	02-05-1998	Bergler et al.	Drawings	
	f2	HK 1063994				T
	f3	HK 1063995				T
	f4	JP2004246720	09-02-2004		Drawings	
	f5	WO99 052051	10-14-1999	International Business Machines		T
	f6	WO99 038062	07-29-1999	Kobil Computer GMBH	Abs.(Engl), Dwg.	
	f7	WO00 036252	06-22-2000	Jacob	Abs.(Engl), Dwg.	
	f8	WO00 042491	07-20-2000	Rainbow Technologies, Inc.		T
	f9	WO00 065180	11-02-2000	Muller et al.	Abs.(Engl), Dwg.	
	f10	WO00 075755	12-14-2000	Eutron Infosecurities		T
	f11	WO01 014179	03-01-2001	Wittwer et al.	Abs.(Engl), Dwg.	
	f12	WO01 038673	03-31-2001	Wittwer et al.	Abs.(Engl), Dwg.	
	f13	WO01 039102	11-02-2001	Muller et al.		T
	f14	WO01 048339	07-05-2001	Jacob et al.	Abs.(Engl), Dwg.	
	f15	WO01 048342	07-05-2001	Jacob et al.	Abs.(Engl), Dwg.	
	f16	WO01 061692	08-23-2001	Trek Technology		T
	f17	WO01 088693	11-22-2001	Seysen	Abs.(Engl), Dwg.	
	f18	WO01 096990	12-20-2001	Rainbow Technologies, Inc.		T
	f19	WO03 014887	02-20-2003	Activcard Ireland		T
	f20	WO03 034189	04-23-2003	Activcard Ireland		T
	f21	WO04 002058	12-31-2003	Gemplus	Abs.(Engl), Dwg.	
	f22	WO04 081706	09-23-2004	Digisafe Ltd.		T
	f23	WO04 081769	09-24-2004	Axalto SA		T

NON PATENT LITERATURE DOCUMENTS

Exam. Initials	Cite No.	Name of author (ALL-CAPS), title of article, title of item, date, pages, vol-issue #, publisher, city and/or country where published.	T
	1	*ACR38CT Contactless SIM Tracker Technical Specification*, Advanced Card Systems Ltd., Hong Kong.	T
	2	*ACR38DT Dual Key Technical Specifications, Version 1.3*, September 2004, Advanced Card Systems Ltd., Hong Kong.	T
	3	*Dallas Semiconductor DS1490F 2-in-1 Fob*, Dallas Semiconductor, Dallas TX.	T

substitute forms PTO/SB/08a & PTO/SB/08b **INFORMATION DISCLOSURE STATEMENT BY APPLICANT**	Application Number	**10/990,296**
	Filing Date	**November 16, 2004**
	First Named Inventor	Dennis J. Ryan
	Art Unit	2876
	Examiner Name	Uyen Chau N. Lee
Sheet 3 OF 3	Practitioner Docket No.	Ryan C-4

NON PATENT LITERATURE DOCUMENTS

Exam. Initials	Cite No.	Name of author (ALL-CAPS), title of article, title of item, date, pages, vol-issue #, publisher, city and/or country where published.	T
	4	*Dallas Semiconductor DS9490-DS9490R USB to 1-Wire/iButton Adaptor*, Maxim I-C, Sunnyvale CA.	T
	5	HARA, YOSHIKO, *Matsushita blends FERAM technology with smart cards*, October 1, 2004, CMP Media, Manhasset NY.	T
	6	*Japan's Matsushita developing memory cards with smart chip function*, October 1, 2004, Mercury News, San Jose CA.	T
	7	*OTi-6828 Flash Disk Controller*, Ours Technology Inc., Taiwan.	T
	8	*Panasonic Develops RFID smartSD Card*, October 4, 2004, Palminfocenter.com, Sunnyvale CA.	T
	9	*Panasonic Develops Industry's First SD Memory Card with Contacless Smart Card Capabilities*, October 1, 2004, The Japan Corporate News Network, Tokyo.	T
	10	ROJAS, PETER, *Panasonic's Smart SD adds RFID to the mix*, October 4, 2004, Engadget LLC, New York NY.	T
	11	*Delivering ultimate security, high performance and ultra low power consumption, SmartMX is now in volume supply*, November 18-20, 2003, Cartes 2003, aris Nort Villepinte, France	T
	12	BALABAN, DAN, *Digital Rights pits SIMS against Flash Cards, Card Technology*, November 2004, pp 24-30, Card Technology, Chicago IL.	T
	13	*P5CT072 Secure Dual Interface PKI Smart Card Controller, Rev. 1.3*, October 2004, Koninklijke Philips Electronics, The Netherlands	T
	14	*Vodafone KK Develops Contactless Smart Card Mobile Handset*, May 6, 2004, HiTEK Magazine, Dubai	T
	15	*SmartSD Card Structure*	T

Examiner Signature

Date Considered

ARTIFACT SHEET

Enter artifact number below. Artifact number is application number + artifact type code (see list below) + sequential letter (A, B, C ...). The first artifact folder for an artifact type receives the letter A, the second B, etc.. Examples: 59123456PA, 59123456PB, 59123456ZA, 59123456ZB

10990296UA

Indicate quantity of a single type of artifact received but not scanned. Create individual artifact folder/box and artifact number for each Artifact Type.

[1] CD(s) containing:

computer program listing □
Doc Code: Computer Artifact Type Code: P

pages of specification
and/or sequence listing □
and/or table
Doc Code: Artifact Artifact Type Code: S

content unspecified or combined ☑
Doc Code: Artifact Artifact Type Code: U

□ Stapled Set(s) Color Documents or B/W Photographs
Doc Code: Artifact Artifact Type Code: C

□ Microfilm(s)
Doc Code: Artifact Artifact Type Code: F

□ Video tape(s)
Doc Code: Artifact Artifact Type Code: V

□ Model(s)
Doc Code: Artifact Artifact Type Code: M

□ Bound Document(s)
Doc Code: Artifact Artifact Type Code: B

□ Confidential Information Disclosure Statement or Other Documents marked Proprietary, Trade Secrets, Subject to Protective Order, Material Submitted under MPEP 724.02, etc.
Doc Code: Artifact Artifact Type Code X

□ Other, description: ______________________
Doc Code: Artifact Artifact Type Code: Z

March 8, 2004

Please forward to Group Art Unit 2876

Amended Compact Discs

EXAMINER NOTE: THIS PAPER IS AN INTERNAL WORKSHEET ONLY. DO NOT ENCLOSE WITH ANY COMMUNICATION TO THE APPLICANT. ITS PURPOSE IS ONLY THAT OF AN AID IN HIGHLIGHTING A PARTICULAR PROBLEM IN A COMPACT DISC.

THE ATTACHED CD (COPY 1) HAS BEEN REVIEWED BY OIPE FOR COMPLIANCE WITH 37 CFR 1.52(E). ***Please match this CD with the application listed below.***

Date: 10-11-2005
Serial No./Control No. 10-990296
Reviewed By: K.SMITH Phone: 308 9210 ext.118

□ The compact discs are readable and acceptable.

□ Copy 1 and Copy 2 of the compact discs are not the same.

□ The compact discs are unreadable.

□ The files on the compact discs are not in ASCII.

□ The compact discs contain at least one virus.

☑ Other
NOT PROPER SUBJECT MATTER FOR CD

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Ryan, et al. Confirmation Number: 2050

Title: MULTI-INTERFACE COMPACT PERSONAL TOKEN APPARATUS AND METHODS OF USE

Serial Number: 10/990,296 Publication No. 20050109841

Filing Date: 11/16/2004 Publication Date 5/26/2005

Docket No.: Ryan C-4

Examiner: Le, Uyen Chau N. Art Unit: 2876

November 14, 2005

By Fax 571-273-8300

COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

AMENDMENT

This is in response to an Office action dated 07/12/2005. A response was due 10/12/2005.

A fee ($60) for a one month's extension of time in which to respond is enclosed herewith.

Please amend the referenced application as follows:

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

Amendments to the Claims are reflected in the listing of claims which begins on page 3 of this paper.

Amendments to the Drawings .... none

Remarks/Arguments begin on page 13 of this paper.

Amendments to the Specification:

At page 1, lines 4-5 (entire paragraph)

This is a non-provisional filing based on USSN 60/520,698 filed 11/17/2003 by Ryan, Comiskey, ~~and~~ Knapich and Finn.

Amendments to the Claims:

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

Listing of Claims:

1. (original) A compact personal token apparatus, comprising:
a connection module;
a translation module;
a processor module; and
an input/output module.

2. (currently amended) The compact personal token apparatus of claim 1, wherein:
the connection module is for interfacing the personal token apparatus with [[a]] an Internet-capable appliance; and
the interface is selected from the group consisting of USB, FireWire, IR, Bluetooth, standard serial port, WLAN.

3. (currently amended) The compact personal token apparatus of claim 1, wherein:
the connection module is for interfacing the personal token apparatus with [[a]] an Internet-capable appliance; and
the Internet-capable appliance comprises a device selected from the group consisting of personal computer (PC), laptop, PDA, MP3 player and cellphone.

4. (original) The compact personal token apparatus of claim 1, wherein:
the translation module moves signals between a USB interface and a smart card interface.

5. (currently amended) The compact personal token apparatus of claim 4, wherein:
the smart card interface is selected from the group consisting of ISO 7816, ISO 14443 (RFID-contactless interface) and ISO 15693 (RFID-contactless interface) .

6. (original) The compact personal token apparatus of claim 1, wherein:
the processor module comprises a dual interface (DI) chip.

7. (original) The compact personal token apparatus of claim 1, wherein:
the processor module incorporates the translation module.

8. (original) The compact personal token apparatus of claim 1, wherein:
the output module comprises an RF antenna and a modulator.

9. (original) The compact personal token apparatus of claim 1, further comprising:
flash memory.

10. (currently amended) The compact personal token apparatus of claim 1, wherein:
the translation module moves ~~signals between a USB interface and a wireless interface~~ data or signals from a USB interface to an RFID interface and a wireless interface with storage of data in a flash memory or EEPROM of the processor module (dual interface chip), and data can reside temporarily at one of the interfaces.

11. (currently amended) The compact personal token apparatus of claim 1, wherein:
the translation module is incorporated in the processor module ~~to that the device~~ so that the personal token apparatus can go directly from USB to wireless (including RFID) without being limited by smart card software architecture limitations.

12. (currently amended) The compact personal token apparatus of claim 1, wherein:
the connection, translation, processor and input/output modules are embodied in ~~the~~ a form of an apparatus having ~~the~~ a general physical configuration of a conventional USB memory fob.

13. (original) The compact personal token apparatus of claim 12, wherein the fob comprises;
a first physical module containing the input module and the translation module; and
a second physical module containing the processor module and the output module.

14. (original) The compact personal token apparatus of claim 1, wherein:
the output module comprises contacts for interfacing with a smart card.

15. (currently amended) The compact personal token apparatus of claim 1, wherein:
the fob is ~~capable of~~ configured for interfacing with the Internet and emulating a smart card.

16. (currently amended) The compact personal token apparatus of claim 1, wherein:
the connection module is for interfacing the personal token apparatus with an Internet-capable appliance; and further comprising:
an input module is for connecting to the Internet; and
the personal token apparatus incorporates firewall functionality to protect the Internet-capable ~~applicance~~ appliance.

17. (original) The compact personal token apparatus of claim 1, further comprising:
interfaces for ISO contact, contactless, USB and DSL.

18. (original) The compact personal token apparatus of claim 1, further comprising:
an LCD screen.

19. (original) The compact personal token apparatus of claim 1, further comprising:
at least one switch.

20. (original) The compact personal token apparatus of claim 1, further comprising:
at least one LED.

21. (original) A compact personal token apparatus comprising:
a standard–compliant contact based interface, the contact based interface complying to at least one standard interface selected from the group consisting of USB, IEEE 1394, PCMCIA,

Amendments to the Claims:

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

Listing of Claims:

1. (original) A compact personal token apparatus, comprising:
a connection module;
a translation module;
a processor module; and
an input/output module.

2. (currently amended) The compact personal token apparatus of claim 1, wherein:
the connection module is for interfacing the personal token apparatus with [[a]] an Internet-capable appliance; and
the interface is selected from the group consisting of USB, FireWire, IR, Bluetooth, standard serial port, WLAN.

3. (currently amended) The compact personal token apparatus of claim 1, wherein:
the connection module is for interfacing the personal token apparatus with [[a]] an Internet-capable appliance; and
the Internet-capable appliance comprises a device selected from the group consisting of personal computer (PC), laptop, PDA, MP3 player and cellphone.

4. (original) The compact personal token apparatus of claim 1, wherein:
the translation module moves signals between a USB interface and a smart card interface.

5. (currently amended) The compact personal token apparatus of claim 4, wherein:
the smart card interface is selected from the group consisting of ISO 7816, ISO 14443 <u>(RFID-contactless interface)</u> and ISO 15693 <u>(RFID-contactless interface)</u> .

Compact Flash, Multi Media, Memory Stick, Smart Media, Secure Digital, mini SD, IBM Micro Drive, and any similar standard interface.

22. (currently amended) The compact personal token apparatus of claim 21, further comprising:

a standard–compliant contactless/wireless interface; the contactless/wireless interface complying to one or more of the following standard interfaces: wireless interface, RFID-contactless interface according to ISO 14443 and ISO 15693 as well as similar interfaces, Bluetooth compatible interface, WLAN 812.11, UWB, and any similar interface.

23. (currently amended) The compact personal token apparatus of claim 22, further comprising:

a standard-compliant interface releaseably coupleable to a host processing device, this being under ~~the~~ a command of an operating system;

an interface module providing translation of standard-compliant contact based interface messages via a memory chip to Bluetooth /WLAN 812.11 device compatible compliant messages, and providing the translation of Bluetooth /WLAN 812.11 device compliant messages via a memory chip to standard-compliant contact based interface messages; and

a Bluetooth /WLAN 812.11 device having a Bluetooth/WLAN 812.11 compliant interface communicating through the interface module with the host processing device via a memory chip; the same Bluetooth /WLAN 812.11 device communicating through ~~its~~ a Bluetooth /WLAN 812.11 compatible interface.

24. (currently amended) The compact personal token apparatus of claim 23, wherein:

the contactless / wireless ~~module~~ interface is releaseably coupleable from the ~~Interface~~ interface module.

25. (original) The compact personal token apparatus of claim 22, further comprising:

a processor module; and

additional memory selected from the group consisting of flash memory and EEPROM device powered and addressed by the processor module;

wherein the additional memory can be used for user authentication and to run applications.

26. (original) The compact personal token apparatus of claim 22, further comprising:

a standard–compliant smart card contact interface complying to ISO 7816, or any similar interface.

27. (currently amended) The compact personal token apparatus of claim 22, further comprising:

a processor module, preparing messages to be sent by the contactless/wireless interface [[of]] and interpreting messages received via the interface.

28. (currently amended) The compact personal token apparatus of claim 21, further comprising:

a standard-compliant interface releaseably coupleable to a host processing device, this being under [[the]] a command of an operating system;

an interface module providing translation of standard-compliant contact based interface messages to ISO 7816 compliant messages and providing the translation of ISO 7816 compliant messages to standard-compliant contact based interface messages;

a dual interface processor having an ISO7816 compliant interface communicating through the interface module with the host processing device, the dual interface processor communicating through an RFID-contactless interface and connected to an inductive antenna.

29. (currently amended) The compact personal token apparatus of claim 28, wherein:

the contactless / wireless ~~module~~ interface is releaseably coupleable from the ~~Interface~~ interface module.

30. (currently amended) The compact personal token apparatus of claim 28, wherein:

the dual interface processor is mounted in a dual interface card complying to ISO 7810 or a 7816 compliant SIM module and connected norms;

the compact personal token apparatus provides physical contacts for the dual interface card, or a 7816 compliant form factor; and

when connected, the dual interface or SIM card can communicate with the host processing device through the interface module inside the personal token apparatus and, once the communication is done, the card can be released from the personal token apparatus and can be used then in the real world.

31. (currently amended) The compact personal token apparatus of claim 28, wherein:

the dual interface chip (processor) inside the personal token apparatus can be directly programmed by a software running on the host system using the interface processor without the need for an external contact based dual interface read/write device.

32. (currently amended) The compact personal token apparatus of claim 31, wherein:

~~the downloaded information can be used in the real world by using the contactless RFID interface~~

the software is web based, allowing for downloading information from the web directly into the dual interface processor memory, thus linking the virtual world to the real world.

33. (currently amended) The compact personal token apparatus of claim ~~31~~ 32, wherein:

~~the software is web based, allowing for downloading information from the web directly into the dual interface processor memory (for example, event tickets) thus linking the virtual world to the real world~~

the downloaded information can be used in the real world by using the contactless RFID interface.

34. (original) The compact personal token apparatus of claim 33, wherein:

the downloaded information can be used in the real world by using the contactless RFID interface.

35. (currently amended) The compact personal token apparatus of claim 33, wherein:

the information stored in the personal token apparatus via the standard contact based interface is used for personal identification, secure network logon, access control, e-ticketing, e-payment and similar applications using either the standard compliant interface or the RFID-compliant interface.

36. (currently amended) The compact personal token apparatus of claim 33, wherein:

information received through the RFID- interface can be stored in the memory of the personal token apparatus and can then be provided to the host processing device via the standard interface, thus allowing a complete information exchange between the virtual world and the real world.

37. (currently amended) The compact personal token apparatus of claim 31, wherein:

the information stored in the personal token apparatus via the standard contact based interface is used for personal identification, secure network logon, access control, e-ticketing, e-payment and similar applications using either the standard compliant interface or the RFID-compliant interface.

38. (currently amended) The compact personal token apparatus of claim 31, wherein:

information received through the RFID- interface can be stored in the memory of the personal token apparatus and can then be provided to the host processing device via the standard interface, thus allowing a complete information exchange between the virtual world and the real world.

39. (original) The compact personal token apparatus of claim 31, further comprising:

additional memory selected from the group consisting of flash memory and EEPROM device powered and addressed by the processor module;

wherein the additional memory can be used for user authentication and to run applications.

40. (currently amended) The compact personal token apparatus of claim 21, further comprising:

a standard-compliant interface releaseably coupleable to a host processing device, this being under ~~the~~ a command of an operating system;

an interface module providing translation of standard-compliant contact based interface messages via a memory chip to Bluetooth /WLAN 812.11 device compatible compliant messages, and providing the translation of Bluetooth /WLAN 812.11 device compliant messages via a memory chip to standard-compliant contact based interface messages; and

a Bluetooth /WLAN 812.11 device having a Bluetooth/WLAN 812.11 compliant interface communicating through the interface module with the host processing device via a memory chip; the same Bluetooth /WLAN 812.11 device communicating through its Bluetooth /WLAN 812.11 compatible interface.

41. (original) The compact personal token apparatus of claim 21, further comprising:

a processor module; and

additional memory selected from the group consisting of flash memory and EEPROM device powered and addressed by the processor module;

wherein the additional memory can be used for user authentication and to run applications.

42. (original) The compact personal token apparatus of claim 21, further comprising:

a standard–compliant smart card contact interface complying to ISO 7816, or any similar interface.

43. (currently amended) The compact personal token apparatus of claim 21, further comprising:

a connection module, connecting the personal token apparatus to a host device ~~such as~~ including PC, PDA, smart cellular phone or similar device, either directly or with the help of a standard reader device such as a memory card reader.

44. (currently amended) The compact personal token apparatus of claim 21, further comprising:

a standard-compliant interface releaseably coupleable to a host processing device, this being under ~~the~~ a command of an operating system; and

a translation module, translating messages incoming from the contact based interface, and translating messages to the host device from the personal token apparatus.

45. (currently amended) The compact personal token apparatus of claim 21, further comprising:

a triple interface ~~(e.g., contact, contactless, USB)~~ processor including contact, contactless, USB.

46. (currently amended) Method of interacting wirelessly, comprising:

providing a device;

interfacing the device with [[a]] an Internet-capable appliance; and

providing a smart card interface in the device.

47. (original) Method, according to claim 46, wherein:

the interface with the Internet-capable appliance is selected from the group consisting of USB, FireWire, IR, Bluetooth, standard serial port, WLAN.

48. (original) Method, according to claim 46, wherein:

the Internet-capable appliance comprises a device selected from the group consisting of personal computer (PC), laptop, PDA, MP3 player and cell phone.

49. (original) Method, according to claim 46, wherein:

the smart card interface is selected from the group consisting of ISO 7816, ISO 14443 and ISO 15693.

50. (original) Method, according to claim 46, wherein:

the device is modular in construction.

51. (currently amended) Method, according to claim 46, wherein:

the device performs a firewall functionality to protect the Internet-capable ~~applicance~~ appliance.

52. (original) Method, according to claim 46, wherein:

the device incorporates interfaces for ISO contact, contactless, USB and DSL.

Responding to the Office action

This is in response to an Office action dated 7/12/2005.

A response is due 10/12/2005, and can be extended.

A one month extension of time is required and requested. November 12th is a Saturday.

Status of the Claims

Claims 1-52 are pending.

Claims 1-52 are rejected.

Inventorship

Please note that this application claimed priority of three provisional applications, as follows:

- This is a non-provisional filing based on USSN 60/520,698 filed 11/17/2003 by Ryan, Comiskey and Knapich.
- This is a non-provisional filing based on USSN 60/562,204 filed 4/14/2004 by Comiskey, ***Finn*** and Ryan.
- This is a non-provisional filing based on USSN 60/602,595 filed 8/18/2004 by ***Finn***.

Recently, the inventorship in the first provisional (60/520,698) was amended to include ***Finn***. (Corrected Filing Receipt mailed 10/03/2005)

The Specification (page 1, cross-references) is amended, accordingly.

Information Disclosure

Recently, an Information Disclosure Statement was filed, along with the appropriate fee. (return postcard stamped Sep 12, 2005)

Claim Objections

Numerous objections were noted by the Examiner, with suggested substitutions.

The claims have been amended per the Examiner's suggestions.

35 USC §112, second paragraph

Claim 32, line 2, regarding "the downloaded information" lacks antecedent basis.

Claims 32 and 33 have been effectively "reversed", and claim 33 now depends from claim 32.

Substantive Grounds of Rejection

The prior art being relied upon is:

US 6,748,541 (Margalit)

US 2003/0236821 (Jiau)

Claims 1-7, 9, 12-16, 21, 41-44 and 46-51 are rejected under 35 U.S.C. 102(e) as being anticipated by Margalit et al (US 6,748,541). The Examiner states the following:

> Re claims 1-7, 9, 12-16, 21, 41-44 and 46-51: Margalit et al discloses a compact personal token apparatus 125, comprising; a connection module 140; a translation module, which incorporated with a processor module 130; and an input/output module (fig. 2); wherein: the connection module 140 is for interfacing the personal token apparatus with a an Internet-capable appliance; and the interface is a USB interface (fig. 2); wherein: the connection module 140 is for interfacing the personal token apparatus with a an Internet-capable appliance; and the Internet-capable appliance comprises a device, which is a personal computer (PC); wherein: the translation module moves signals between a USB interface and a smart card interface (fig. 2; col. 5, lines 1-30); wherein: the smart card interface 170 is an ISO 7816; wherein: the processor module 130 comprises a dual interface (DI) chip (i.e., USB and smart card); wherein: the processor module 130 incorporates the translation module (i.e., for passing data from the smart card to the USB interface chip 140 and vice versa) (fig. 2; col. 5, lines 20-27); flash memory 150 (fig. 2; col. 4, lines 35-38); a first physical module containing the input module and the translation module; and a second physical module containing the processor module and the output module (fig. 3); wherein: the connection, translation, processor, and input/output modules are embodied in a form of an apparatus having a general physical configuration of a conventional USB memory fob (figs. 3-5B); wherein: the output module comprises contacts for interfacing with a smart card (fig. 2); the fob is configured for interfacing with the Internet and emulating a smart card (fig. 2); wherein: the connection module 140 is for interfacing the personal token apparatus with an Internet-capable appliance; and further comprising: an input module is for connecting to the Internet; and the apparatus incorporates firewall functionality to protect the Internet-capable appliance (i.e., login process including username and password) (fig. 5B); a standard-compliant contact based interface, the contact based interface complying to at least one standard interface selected from the group consisting of USB, IEEE 1394, PCMCIA, Compact Flash, Multi Media, Memory Stick, Smart Media, Secure Digital, mini SD, IBM Micro Drive, and any similar standard interface (fig. 2).

Claims 1, 8, 10, 11, 18-29 and 31-40 are rejected under 35 U.S.C. 102(e) as being anticipated by Jiau (US 2003/0236821 Al). The Examiner states the following:

> Re claims 1, 8, 10, 11, 18-29 and 31-40: Jiau discloses a compact personal token apparatus 1, comprising: a connection module 1312 (paragraph [0044]); a translation module, which incorporated with a processor module 132; and an input/output module [139, 1341, 1342, 1343, 13441 (figs. 1 & 3A-3C); the translation module moves signals between a USB interface and a wireless interface (paragraphs [0050-0051]); an LCD screen 1341 and LEDs 1342 (fig. 3C); a standard-compliant contact based interface, the contact based interface complying to at least one standard interface selected from the group consisting of USB, IEEE 1394, PCMCIA, Compact Flash, Multi Media, Memory Stick, Smart Media, Secure Digital, mini SD, IBM Micro Drive, and any similar standard interface (paragraph [0044]); a standard-compliant contactless/wireless interface 1311; the contactless/wireless interface 1311 complying to one or more of the following standard interfaces: RFID-contactless interface according to WLAN 812.11 and Bluetooth compatible interface (paragraphs [0047] & [0050]); a flash memory 133 (fig. 3A); wherein: the dual interface chip (processor) inside the personal token can be directly programmed by a software running on the host system using the interface processor without the need for an external contact based dual interface read/write device (paragraph [0052]); wherein: the downloaded information can be used in the real world; wherein: the software is web based, allowing for downloading information from the web directly into the dual interface processor memory thus linking the virtual world to the real world (paragraph [0052]); wherein: the information stored in the personal token via, the standard contact based interface is used for personal identification, secure network logon, access control, e-ticketing, e-payment and similar applications using either the standard compliant interface or the RFID-compliant interface (paragraph [0067]).

Claims 17, 45 and 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Margalit et al in view of Jiau. The Examiner states the following:

> Re claims 17, 45 and 52: Margalit et al has been discussed above but is silent with respect to a contactless interface.
>
> Jiau teaches a communication unit 131 includes wireless connection 1311 (fig. 3B; paragraph [0051]).
>
> It would have been obvious to an artisan of ordinary skill in the art at the time the invention was made to incorporate a wireless connection of Jiau into the system taught by Margalit et al in order to provide Margalit et al with a universal system wherein the system can be utilized in any type of communications (i.e., contact, contactless, USB, etc.). Furthermore, such modification would provide the user the flexibility in using the system wherein the user does not have to concern about whether or not the system is compatible with a particular communication system that the user intend to use, and therefore an obvious expedient.

Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jiau in view of Margalit et al. The Examiner states the following:

Re claim 30: Jiau has been discussed above but is silent with respect to an interface that is complying to ISO 7810 or a 7816 compliant SIM module.

Margalit et al teaches a personal token apparatus 125 having an interface that is a 7816 compliant SIM module (fig. 2).

It would have been obvious to an artisan of ordinary skill in the art at the time the invention was made to incorporate a 7816 compliant SIM module of Margalit et al into the system as taught by Jiau in order to provide Jiau with a universal system wherein the system can be utilized in any type of communications (i.e., contact, contactless, USB, etc.). Furthermore, such modification would provide the user the flexibility in using the system wherein the user does not have to concern about whether or not the system is compatible with a particular communication system that the user intend to use, and therefore an obvious expedient.

The Cited References, Generally

US 6,748,541 (Margalit) discloses user-computer interaction method for use by a population of flexibly connectable computer systems and a population of mobile users, the method comprising storing information characterizing each mobile user on an FCCS plug to be borne by that mobile user; and accepting the FCCS plug from the mobile user for connection to one of the flexibly connectible computer systems and employing the information characterizing the mobile user to perform at least one computer operation.

In Margalit, mention is made of "smart card", in the summary/glossary section (column 3, line 30). (The term "smart card" refers to a typically plastic card in which is embedded a chip which interacts with a reader, thereby allowing a mobile bearer of the smart card to interact with a machine in which is installed a smart card reader, typically with any of a network of machines of this type.)

Although mentioning "smart card", no mention is made by Margalit to a contactless interface or any suggestion thereof.

Compare, for example, the following statement by Margalit: "A particular feature of the USB plug device of FIG. 1 is that it has data storage capabilities and is thus analogous to a memory smart card." (column 4, line 20)

See also Margalit at column 5, line 1: "FIG. 2 is a simplified block diagram of a USB plug device, constructed and operative in accordance with a preferred embodiment of the present invention, which is a one-piece smart card reader and smart card chip preferably providing both secured storage and cryptographic capabilities."

See also Margalit at column 5, line 20:

> The USB interface chip 140 gets USB packets from the USB host 120. The USB interface chip 140 parses the data and passes it to the microprocessor 130. The data, which typically comprises a ISO7816-3 T=0/1 formatted packet, is passed by the microprocessor to the smart-card 170 in a ISO7816-3 protocol. The microprocessor 130 gets the response from the smart card 160 and passes the data to the USB interface chip 140. The USB interface chip 140 wraps the data in USB packet format and passes it to the host 120.
>
> A particular advantage of the embodiment of FIG. 2 is that smart card functionality is provided but there is no need for a dedicated reader because the plug 110 is connected directly to a USB socket in the host 120.

See also Margalit at column 7, line 5:

> Smart card functionalities which are preferably provided by the FCCS plug of the present invention include:
>
> 1. Controlling access to computer networks: Smart card or plug has ID information, network authenticates and allows access on that basis. Authentication may be based upon "what you have", "what you are" e.g. biometric information and "what you know" (e.g. password).
>
> 2. Digital signatures or certificates for verifying or authenticating the identity of the sender of a document.
>
> 3. Storage of confidential information e.g. medical information. A smart card or plug may store confidential information and interact with a network which does not store the confidential information.

Margalit is assigned to Alladin Knowledge Systems, Ltd. An example of the end product can be found at http://www.aladdin.com/etoken/usb_device.asp

In Margalit, no mention is made to a contactless interface or any suggestion thereof.

US 2003/0236821 (Jiau) discloses body wearable personal network server and system. A body wearable personal network server device has a display, function keys, alarm output indicators, a disk driver to receive and store clients' data, and communication devices to communicate to its clients, such as mobile phone, personal digital assistant (PDA), personal computer, and notebook computer. A body wearable personal network device also contains software modules; such as a protocol handler to handle Internet based protocols XML/FTP/HTTP/TCP/IP, diagnostic system to automatically transmit of notification messages to its clients, and various applications to provide various services for its clients. A body wearable personal network device has gateway functionality between PAN (using Bluetooth) and WLAN (using IEEE802.11b).

The following numbered paragraphs (44, 47, 50, 51, 52 & 67) from Jiau are specifically cited by the Examiner:

> [0044] FIG. 1A illustrates the general working environment of the present invention where it is applied. The device of the present invention denoted as 1 is a body wearable device, and is able to communicate with personal communicators, such as mobile phone denoted as 2, PDA denoted as 3, personal computer denoted as 4, and notebook computer denoted as 5, via a wireless connection; such as a PC card (formerly known as PCMCIA card--The Personal Computer Memory Card International Association) providing IEEE 802.11 or Bluetooth protocol in a PC card slot, or/and a wire connection through USB connector. In order to achieve the functions of the present invention, the proper software needs to be installed in the device of the present invention 1, and in the personal communicators 2, 3, 4, and 5.
>
> [0047] FIG. 1C shows that the BWPNS denoted as 1 provides the gate way functionality between PAN (through protocol; such as Bluetooth), and WLAN (through protocol; such as IEEE802.11b).
>
> [0050] As illustrated in FIG. 2D, the BWPNS device is designed for providing wire and wireless connections. The wire connection is the USB type of adaptor denoted as 121, which is able to connect to a client via USB cable denoted as 122. The wireless connection use a Bluetooth plus IEEE802.11b card build inside device 6, which can adopt dual-mode Bluetooth and IEEE802.11b in the same device; such as Blue802 Technology unveiled by Intersil and Silicon Wave. Contact information is Silicon Wave, Inc. 6256 Greenwich Drive Suite 400, San Diego, Calif. 92122 and Intersil Corporation, 7585 Irvine Center Drive Suite 100, Irvine, Calif. 92618. A battery release button denoted as 119 to release the removable battery, which is locked through the notch denoted as 120. The power supply contacts denoted as 118. The speaker apparatus denoted as 124, which is programmable and allows application programs to use it to generate basic radio alarms.

In Jiau [0050], the body wearable personal network server (BWPNS) device is designed for providing wire and wireless connections. The wire connection is the USB type of adapter denoted as 121, which is able to connect to a client via a USB cable denoted as 122. The wireless connection uses a Bluetooth plus IEEE 802.11b card build inside the device 6, which can adopt dual-mode Bluetooth and IEEE 802.11b in the same device. Looking at the website of Suncore, www.suncore.com.tw, it can be recognised that the above description is a dual mode wireless adapter.

[0051] A block diagram FIG. 3A illustrates the primary components to comprise the BWPNS hardware portion 21 of the server 1 in FIG. 1B. The components include MPU (MicroProcessor Unit) 132, power supply 138, ROM and RAM memory 135, output devices 134, Flash Memory Chips; (Disk-on-Chips) 133, the communication units 131, function key entry 139, and a timer 136. The communication units illustrated in FIG. 3B include wireless connection 1311, providing dual radio modes of PAN (such as Bluetooth) plus WLAN (such as IEEE 802.11b) via a PC card or build-in device, and USB wire communication port 1312. The output devices illustrated in FIG. 3C include a LCD 1341, indication LEDs 1342, a speaker 1343, and a vibrated device 1344.

[0052] A block diagram FIG. 4A illustrates the software hierarchical structure for software portion 22 in FIG. 1B in the BWPNS denoted as 1 in FIG. 1B. The device drivers 241 interface with hardware devices and provide the upper level the software channels to use hardware devices, such as to access hard disk driver for retrieving or storing data files. An operating system (OS) 242 is a brain of the software portion, which handles and manages system resources, schedules application tasks, manages memory allocation, handles system exceptions, and so on. The HTTP/TCP/IP/Data Link/Physical Layer protocol handler 243 performs all protocol issues according to protocol agreements published by the standard organizations; such as ITU or IETF. Based on the customer's requirements, profiles or the incoming event type, the XML (Extensible Markup Language) handler 244 or FTP (File Transfer Protocol) handler 245 is evoked for receiving or sending the proper types of presentations. The data formatter 246 is the extension of the applications, which convert data into proper format according to users' profiles. As FIG. 4C, the generated data formats that the BWPNS supports are audio data 221, such as wav files, music data 222, such asmp3 files, binary data 223, control data 224, which is under the control command format using between server and clients, text data 225, image data 226, such as JEPG, web data 227, such as WAP, XML files, game data 228, movie data 229, such as mpeg files, and library data 230, such as dll files.

[0067] FIG. 5 is a data flow diagram that illustrates the software portion 22 in FIG. 1B in the BWPNS denoted as 1 in FIG. 1B. The communication reception unit 151 receives an event sent from a client (a personal communicator), or from the function key touch pad on the BWPNS. The communication reception unit forwards the event to the security-checking unit 153 for the security and authorization checking. If the incoming event does not pass the security checking, a failure indication signal will be sent back to the event generator via the communication transmission unit 152. If the incoming event passes the checking, the event is sent to the signal management unit 154 for distinguishing the type of the event in order to determine the further direction of the event. If the event is sent from the personal communicator, the signal confirmation unit 155 will be evoked to send a confirmation message back to the personal communicator via the communication transmission unit 152, otherwise based on the event type, a proper event handler unit is evoked to handle the incoming event. The general event handlers are: System Command Handler Unit (SCHU) 157: Some of events are for control commands, which are used to control, manage, or synchronize the in progressing communication activities between the server (BWPNS), and clients (Personal Communicators); such as hand sharking activity.

The Invention, Generally

The invention is directed to MULTI-INTERFACE COMPACT PERSONAL TOKEN APPARATUS AND METHODS OF USE. (Title) A compact personal token apparatus, suitably resembling a conventional USB memory fob in size, shape, and form which can be plugged into a PC and interfaced with the virtual world of the Internet. The apparatus is capable of loading and storing information from the Internet, via the PC to its flash memory or EEPROM and then using the stored information or value via its wireless interface in the real world. The apparatus is capable of implementing an auto-run application, when inserted into a personal computer. The apparatus is capable of exchanging information with other devices having compatible interfaces. The apparatus can also function as a firewall when plugged between an Internet connection and a PC. (See Abstract)

More particularly, as described in the Specification (paragraph references from published application),

> [0124] The invention is generally a compact personal token apparatus which can be plugged into a personal computer and interfaced with the virtual world of the Internet. The apparatus (or, as will be evident, a portion of a modular apparatus) can then be removed from the personal computer and used to conduct real world transactions. The compact personal token apparatus is suitably in the general form of a fob, resembling a USB memory fob. The compact personal token apparatus comprises a wireless interface.

The invention is directed to an apparatus incorporating USB, RFID & WLAN interfaces as well as Mass Storage in a single device.

It should be understood, and it is supported, that thoughout the specification, the term "wireless interface" generally (and frequently) refers to RFID (contactless) **and** Wireless (WLAN), in the plural form.

As is known, RFID (i.e. contactless) operates at 13.56 MHz, and Wireless (i.e. WLAN 802.11a/b/g) operates at 2.4 & 5.0 GHz. They are different, but they are both "wireless" in the broad sense of the term. RFID operates at a maximum distance of 1 meter for pure identification and in a payment application, the distance is restricted to 10 cm.

As is clearly set forth in the specification, the apparatus of the present invention can communicate either with the RFID – contactless interface or with the Wireless Interface. The apparatus is constructed to have both. In a derivation of the apparatus, the apparatus also includes Bluetooth (for private area network) which operates at the same frequency as WLAN 802.11 b/g, but in fact is an additional interface.

In summary, the RFID contactless interfaces are ISO 14443, 15693 and NFC, the wireless interfaces are WLAN, Bluetooth and UWB and the mechanical interface is for example USB. The present invention has these interfaces. Additionally, the present invention has a shared memory between the interfaces which can be EEPROM or NAND Flash Memory. The Smart Card interface is an internal configuration where the device of the invention translates USB to Smart card protocol.

> [0129] The invention is generally a compact personal token apparatus which can be by means of standard-compliant interfaces (described hereinbelow) connected to a personal computer and/or other internet capable devices such as; cell phones, personal digital assistants (PDA), digital media players, digital cameras etc. and interfaced with the virtual world of the Internet. The apparatus (or, as will be evident, a portion of a modular apparatus) can then be removed from the personal computer and used to

conduct real world transactions. The compact personal token apparatus is suitably in the general form of a fob, resembling a USB memory fob. In some implementations it will take the general form factor required of the standard compliant interface such as SD and Mini SD cards, Multi Media Cards (MMC), PCMCIA Cards, etc. The compact personal token apparatus generally comprises a **wireless interface**.

Again (in the previous paragraph), the term "wireless interface" refers to RFID (contactless) **and** Wireless (WLAN), in the plural form.

[0131] According to the invention, a compact personal token apparatus comprises a connection module; a translation module; a processor module; and an input/output module. The connection module is for interfacing the personal token apparatus with an Internet-capable appliance; and the interface is selected from the group consisting of USB, FireWire, IR, Bluetooth, standard serial port, WLAN. The Internet-capable appliance may comprise a device selected from the group consisting of personal computer (PC), laptop, PDA, MP3 player and cellphone. The translation module moves signals between a USB interface and a smart card interface. The smart card interface may be selected from the group consisting of ISO 7816, ISO 14443 and ISO 15693.

Here (in the previous paragraph), we specify USB (mechanical interface), WLAN & Bluetooth (wireless interface) and ISO 14443 and ISO 15693 (contactless interface or generic terms RFID)

[0134] The apparatus may further comprise a standard-compliant contactless/wireless interface; the contactless/wireless interface complying to one or more of the following standard interfaces: RFID-contactless interface according to ISO 14443 and ISO 15693 as well as similar interfaces, Bluetooth compatible interface, WLAN 812.11, UWB, and any similar interface.

Paragraph [0134] expresses the contactless/wireless distinction better, and supports the comments made before about "wireless" including either contactless (e.g., RFID) or Wireless (e.g., WLAN)

[0137] The apparatus may further comprise a dual interface chip (processor) inside the personal token which can be directly programmed by a software running on the host system using the interface processor without the need for an external contact based dual interface read/write device. The software may be web based, allowing for downloading information from the web directly into the dual interface processor memory (for example, event tickets) thus linking the virtual world to the real world. The downloaded information may be used in the real world by using the contactless RFID interface.

[0141] The apparatus may further comprise a processor module; and additional memory selected from the group consisting of flash memory and EEPROM device powered and addressed by the processor module; wherein the additional memory can be used for user authentication and to run applications.

[0146] The apparatus may further comprise a triple interface (e.g., contact, contactless, USB) processor.

[0151] The "smart fob" is capable of loading and storing information from the Internet, via a PC or other Internet capable device to its memory and then using the stored information via its wireless interface in the real world. The "smart fob" is also capable of exchanging information with a conventional smart card.

An importance point being made in the prevoius paragraph(s) is the concept of exchanging data from the memory.

Traversing the Rejection

First of all, there is little or no correlation between the technology of the present invention and the technology combination of Margalit and Jiau. The present invention merges RFID with Wireless and incorporates Flash Memory for storage and autorun applications as well as incorporating diverse mechanical connection interfaces. Margalit is attempting to replace contact smart cards with a USB token for the PC environment and Jiau outlines a wireless server client which can communicate with a mobile computing device. Jiau also bridges PAN and WLAN, which in fact is a dual mode WiFi adapter.

Margalit et al (US 6,748,541) and Jiau (US 2003/0236821) do not anticipate the combination of USB, Contactless, Wireless and Extended Memory with Flash. Margalit is focused on a smart card token (for example for an online banking application), while Jiau is focused on a portable server with dual mode wireless interface, namely Bluetooth and WiFi (this apparatus is almost like an Access Point or Router to enable Internet communication with the client, namely a PDA). Neither of them concerns themselves with RFID for logical and physical access as well as authentication and payment. Even combining the teachings of the two references, it is not possible to create the apparatus of the present invention.

The independent claims are directed to...

1. A compact personal token apparatus ...
   (claims 2-20 depend from claim 1)

21. A compact personal token apparatus ...
   (claims 22-45 depend from claim 21)

46. Method of interacting wirelessly ...
   (claims 47-52 depend from claim 46)

Claims 1-7, 9, 12-16, 21, 41-44 and 46-51 are rejected as being anticipated by Margalit.

US Patent 6,748,541 (Margalit) describes a flexible connectable computer system apparatus for use by a population of mobile users. The configuration of the apparatus in it's simplest form includes a USB interface chip, a CPU, user data memory, firmware and a random access memory. By replacing the user data memory by an ISO compliant smart card chip, the apparatus incorporates a USB plug device which is a one-piece smart card reader and smart card chip providing both secured storage and cryptographic capabilities. The USB plug device includes a CPU and a smart card chip memory, typically a ISO7816 (T=0/1) protocol-based chip communicating with the CPU using an ISO7816-3 protocol. The smart card functionalities provided by the apparatus include:

- Digital signature verification and / or controlling access to computer networks
- Storage of confidential information
- Electronic token to authenticate information and / or store passwords or electronic certificates

Margalit's apparatus can also be used for authentication in Virtual Private Networks, extranet and e-commerce.

Claims 5, 6 and 49 differ from Margalit with respect to the contactless interface. Regarding the amendment to claim 5, support may be found in the specification at page 24.

> The apparatus may further comprise a standard–compliant contactless/wireless interface; the contactless/wireless interface complying to one or more of the following standard interfaces: RFID-contactless interface according to ISO 14443 and ISO 15693 as well as similar interfaces, Bluetooth compatible interface, WLAN 812.11, UWB, and any similar interface.

Claims 1, 8, 10, 11, 18-29 and 31-40 are rejected as being anticipated by Jiau.

US 2003/0236821 (Jiau) describes a server-client model of data collection and internet working gateway system. It relates to a body wearable personal network device (server) having gateway functionality between PAN (Personal Area Network using Bluetooth) and WLAN (Wireless Local Area Network using IEEE802.11b). Jiau separates a conventional data communicator device into a server and a client. The server is a body wearable device having its own battery & memory, and able to communicate with the client. The client is a conventional personal communicator such as a mobile telephone, personal digital assistant (PDA), personal computer, pocket personal computer or a notebook. In short, the body wearable personal network device portion is acting as a server and the personal communicators are acting as clients.

Jiau's BWPNS device is designed for providing wire and wireless connections. The wire connection is the USB type of adaptor which is able to connect to a client via a USB cable. The wireless connection avails of a Bluetooth plus IEEE802.11b card, built into the device which can adopt dual mode Bluetooth and IEEE802.11b in the same device.

Jiau relates to an interdependent server-client model whereby the wireless communication is only between the server and the client. There is no mention of communication with the World Wide

Web via a wireless access point with the server. The wireless communication is confined to the server-client model. Furthermore, there is no mention of contactless technology for the purpose of identification and payment.

The sole function of Jiau's BWPNS is to handle some of the computing performed by conventional PDA's and mobile telephones. This fact is highlighted in the background of the invention.

Taking into account the abovementioned, the following can be observed:

Claim 8 is novel over Jiau when referring to the RF antenna in connection with contactless and wireless technology.

Claim 10 is amended herewith to distinguish from a conventional wireless dongle.

Claim 11 is amended herewith to clarify that "wireless" incorporates radio frequency identification (RFID).

Claim 22 See text at specification page 24 (quoted above)

Claim 31 describes a dual interface chip, again relating to radio frequency identification and therefore differs from Jiau.

Claims 32 - 40 are novel over Jiau.

Claims 17, 45 and 52 are rejected as being unpatentable over Margalit in view of Jiau.

Claims 17, 45 and 52 are patentable in light of the comments made above.

Claim 30 is rejected as being unpatentable over Jiau in view of Margalit.

As noted above, there is little or no correlation between the technology of the present invention and the technology combination of Margalit and Jiau. The present invention merges RFID with Wireless and incorporates Flash Memory for storage and autorun applications as well as incorporating diverse mechanical connection interfaces. Margalit is attempting to replace contact smart cards with a USB token for the PC environment and Jiau outlines a wireless server client which can communicate with a mobile computing device. Jiau also bridges PAN and WLAN, which in fact is a dual mode Wi-Fi adapter.

Conclusion

The claims should be allowed.

No new matter is entered by this Amendment.

A fee for a one month's extension of time is enclosed, and the extension is requested.

For the Applicant,

Dwight A. Stauffer Registration No. 47,963

1006 Montford Rd.
Cleveland Hts., OH 44121
216-381-6599 (ph/fax)

CERTIFICATE OF TRANSMISSION BY FACSIMILE

I hereby certify that this correspondence is being transmitted to the United States Patent and Trademark Office (Fax No. 571-273-8300) on November 14, 2005.

Name of Person Signing Certificate : Dwight A. Stauffer

Signature :

Date of Person signing : November 14, 2005

PTO/SB/21 (09-04)
Approved for use through 07/31/2006. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	10/990,296
Filing Date	11 / 16 / 2004
First Named Inventor	Dennis J. Ryan
Art Unit	2876
Examiner Name	Uyen Chau N. Le
Attorney Docket Number	Ryan C-4
Total Number of Pages in This Submission	30

ENCLOSURES *(Check all that apply)*

- ☑ Fee Transmittal Form
  - ☑ Fee Attached
- ☑ Amendment/Reply
  - □ After Final
  - □ Affidavits/declaration(s)
- ☑ Extension of Time Request
- □ Express Abandonment Request
- □ Information Disclosure Statement
- □ Certified Copy of Priority Document(s)
- □ Reply to Missing Parts/ Incomplete Application
  - □ Reply to Missing Parts under 37 CFR 1.52 or 1.53

- □ Drawing(s)
- □ Licensing-related Papers
- □ Petition
- □ Petition to Convert to a Provisional Application
- □ Power of Attorney, Revocation Change of Correspondence Address
- □ Terminal Disclaimer
- □ Request for Refund
- □ CD, Number of CD(s) ____________
  - □ Landscape Table on CD

- □ After Allowance Communication to TC
- □ Appeal Communication to Board of Appeals and Interferences
- □ Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
- □ Proprietary Information
- □ Status Letter
- ☑ Other Enclosure(s) (please Identify below):

PTO-2038 Credit Card Payment Form for payment of $60 extension fee

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name	D.A. STAUFFER PATENT SERVICES LLC		
Signature	DAStauffer		
Printed name	DWIGHT A. STAUFFER		
Date	11/14/05	Reg. No.	47,963

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature	DAStauffer		
Typed or printed name	DWIGHT A. STAUFFER	Date	11/14/05

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

PTO/SB/17 (12-04v2)
Approved for use through 07/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

Effective on 12/08/2004.
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL For FY 2005

☑ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT	($) 60

Complete if Known	
Application Number	10/990,296
Filing Date	11 / 16 / 2004
First Named Inventor	Dennis J. Ryan
Examiner Name	Uyen Chau N. Le
Art Unit	2876
Attorney Docket No.	Ryan C-4

METHOD OF PAYMENT (check all that apply)

□ Check ☑ Credit Card □ Money Order □ None □ Other (please identify): ______

□ Deposit Account Deposit Account Number: ______ Deposit Account Name: ______

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☑ Charge fee(s) indicated below □ Charge fee(s) indicated below, except for the filing fee

☑ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☑ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

	FILING FEES		SEARCH FEES		EXAMINATION FEES		
Application Type	Fee ($)	Small Entity Fee ($)	Fee ($)	Small Entity Fee ($)	Fee ($)	Small Entity Fee ($)	Fees Paid ($)
Utility	300	150	500	250	200	100	______
Design	200	100	100	50	130	65	______
Plant	200	100	300	150	160	80	______
Reissue	300	150	500	250	600	300	______
Provisional	200	100	0	0	0	0	______

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	50	25
Each independent claim over 3 (including Reissues)	200	100
Multiple dependent claims	360	180

Total Claims 52 - 20 or HP = Extra Claims 0 x Fee ($) ______ = Fee Paid ($) ______
HP = highest number of total claims paid for, if greater than 20.

Indep. Claims 3 - 3 or HP = Extra Claims 0 x Fee ($) ______ = Fee Paid ($) ______
HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims
Fee ($) ______ Fee Paid ($) ______

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets ______ - 100 = Extra Sheets ______ / 50 = Number of each additional 50 or fraction thereof ______ (round up to a whole number) x Fee ($) ______ = Fee Paid ($) ______

4. OTHER FEE(S) Fees Paid ($)

Non-English Specification, $130 fee (no small entity discount) ______

Other (e.g., late filing surcharge): one month extension of time fee 60.

SUBMITTED BY

Signature	DAStauffer	Registration No. (Attorney/Agent)	47,963	Telephone	216-381-6599
Name (Print/Type)	DWIGHT A. STAUFFER			Date	11/14/05

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

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

PATENT APPLICATION FEE DETERMINATION RECORD

Effective December 8, 2004

10990296

CLAIMS AS FILED - PART I

	(Column 1)	(Column 2)
TOTAL CLAIMS	52	
FOR	NUMBER FILED	NUMBER EXTRA
TOTAL CHARGEABLE CLAIMS	52 minus 20=	* 32
INDEPENDENT CLAIMS	3 minus 3 =	*
MULTIPLE DEPENDENT CLAIM PRESENT		□

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

SMALL ENTITY TYPE ▭ OR OTHER THAN SMALL ENTITY

RATE	FEE		RATE	FEE
BASIC FEE	395	OR	BASIC FEE	790
X$ 25=	800	OR	X$50=	
X100=		OR	X200=	
+180=		OR	+360=	
TOTAL	1195	OR	TOTAL	

11/14/05 CLAIMS AS AMENDED - PART II

SMALL ENTITY OR OTHER THAN SMALL ENTITY

AMENDMENT A

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	* 52	Minus	** 52	=
Independent	* 3	Minus	*** 3	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				□

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 25=		OR	X$50=	
X100=		OR	X200=	
+180=		OR	+360=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT B

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				□

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 25=		OR	X$50=	
X100=		OR	X200=	
+180=		OR	+360=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT C

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				□

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 25=		OR	X$50=	
X100=		OR	X200=	
+180=		OR	+360=	

CLAIMS ONLY

SERIAL NO. 10/990296

FILING DATE

APPLICANT(S)

11/14/05

CLAIMS

	AS FILED		AFTER 1st AMENDMENT		AFTER 2nd AMENDMENT	
	IND.	DEP.	IND.	DEP.	IND.	DEP.
1	1					
2		|				
3		|				
4		|				
5		|				
6		|				
7		|				
8		|				
9		|				
10		|				
11		|				
12		|				
13		|				
14		|				
15		|				
16		|				
17		|				
18		|				
19		|				
20		|				
21	1					
22		|				
23		|				
24		|				
25		|				
26		|				
27		|				
28		|				
29		|				
30		|				
31		|				
32		|				
33		|				
34		|				
35		|				
36		|				
37		|				
38		|				
39		|				
40		|				
41		|				
42		|				
43		|				
44		|				
45		|				
46	1					
47		|				
48		|				
49		|				
50		|				
TOTAL IND.	3	↲		↲		↲
TOTAL DEP.						
TOTAL CLAIMS		■		■		■

	*		*		*	
	IND.	DEP.	IND.	DEP.	IND.	DEP.
51		|				
52		|				
53						
54						
55						
56						
57						
58						
59						
60						
61						
62						
63						
64						
65						
66						
67						
68						
69						
70						
71						
72						
73						
74						
75						
76						
77						
78						
79						
80						
81						
82						
83						
84						
85						
86						
87						
88						
89						
90						
91						
92						
93						
94						
95						
96						
97						
98						
99						
100						
TOTAL IND.	3	↲		↲		↲
TOTAL DEP.	49					
TOTAL CLAIMS	52	■		■		■

*MAY BE USED FOR ADDITIONAL CLAIMS OR AMENDMENTS

FORM PTO-2022 (1-96)

U.S. DEPARTMENT OF COMMERCE
Patent and Trademark Office

*U.S. Government Printing Office: 1996 - 433-214/70300

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/990,296	11/16/2004	Dennis J. Ryan	Ryan C-4	2050

37053 7590 01/25/2006

D.A. STAUFFER PATENT SERVICES LLC
1006 MONTFORD ROAD
CLEVLAND HTS., OH 44121-2016

EXAMINER	
LE, UYEN CHAU N	
ART UNIT	PAPER NUMBER
2876	

DATE MAILED: 01/25/2006

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

PTO-90C (Rev. 10/03)

Office Action Summary	**Application No.** 10/990,296	**Applicant(s)** RYAN ET AL.	
	Examiner Uyen-Chau N. Le	**Art Unit** 2876	

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

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *14 November 2005*.

2a)☒ This action is **FINAL**. 2b)□ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-52* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-52* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)□ The drawing(s) filed on _____ is/are: a)□ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Prelim. Amdt/Amendment

1. Receipt is acknowledged of the Amendment filed 14 November 2005.

Information Disclosure Statement

2. The information disclosure statement filed 09/12/2005 fails to comply with 37 CFR 1.98(a)(2), which requires a legible copy of each cited foreign patent document; each non-patent literature publication or that portion which caused it to be listed; and all other information or that portion which caused it to be listed. It has been placed in the application file, but the information referred to therein has not been considered.

Claim Rejections - 35 USC § 102

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

> A person shall be entitled to a patent unless -
>
> (e) the invention was described in a patent granted on an application for patent by another filed in the United States before the invention thereof by the applicant for patent, or on an international application by another who has fulfilled the requirements of paragraphs (1), (2), and (4) of section 371(c) of this title before the invention thereof by the applicant for patent.

The changes made to 35 U.S.C. 102(e) by the American Inventors Protection Act of 1999 (AIPA) and the Intellectual Property and High Technology Technical Amendments Act of 2002 do not apply when the reference is a U.S. patent resulting directly or indirectly from an international application filed before November 29, 2000. Therefore, the prior art date of the reference is determined under 35 U.S.C. 102(e) prior to the amendment by the AIPA (pre-AIPA 35 U.S.C. 102(e)).

4. Claims 1-7, 9, 12-16, 21, 41-44 and 46-51 are rejected under 35 U.S.C. 102(e) as being anticipated by Margalit et al (US 6,748,541).

Re claims 1-7, 9, 12-16, 21, 41-44 and 46-51: Margalit et al discloses a compact personal token apparatus 125, comprising; a connection module 140; a translation module, which incorporated with a processor module 130; and an input/output module (fig. 2); wherein: the connection module 140 is for interfacing the personal token apparatus with a an Internet-capable appliance; and the interface is a USB interface (fig. 2); wherein: the connection module 140 is for interfacing the personal token apparatus with a an Internet-capable appliance; and the Internet-capable appliance comprises a device, which is a personal computer (PC); wherein: the translation module moves signals between a USB interface and a smart card interface (fig. 2; col. 5, lines 1-30); wherein: the smart card interface 170 is an ISO 7816; wherein: the processor module 130 comprises a dual interface (DI) chip (i.e., USB and smart card); wherein: the processor module 130 incorporates the translation module (i.e., for passing data from the smart card to the USB interface chip 140 and vice versa) (fig. 2; col. 5, lines 20-27); flash memory 150 (fig. 2; col. 4, lines 35-38); a first physical module containing the input module and the translation module; and a second physical module containing the processor module and the output module (fig. 3); wherein: the connection, translation, processor, and input/output modules are embodied in a form of an apparatus having a general physical configuration of a conventional USB memory fob (figs. 3-5B); wherein: the output module comprises contacts for interfacing with a smart card (fig. 2); the fob is configured for interfacing with the Internet and emulating a smart card (fig. 2); wherein: the connection module 140 is for interfacing the personal token apparatus with an Internet-capable appliance; and further comprising: an input module is for connecting to the Internet; and the apparatus incorporates firewall functionality to protect the Internet-capable appliance (i.e., login process including username and password) (fig. 5B); a standard-compliant contact based interface, the contact based interface complying to at least one standard interface selected from the group consisting of USB, IEEE 1394, PCMCIA, Compact Flash, Multi Media, Memory Stick, Smart Media, Secure Digital, mini SD, IBM Micro Drive, and any similar standard interface (fig. 2).

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

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

6. Claims 1, 8, 18-29 and 31-40 are rejected under 35 U.S.C. 102(e) as being anticipated by Jiau (US 2003/0236821 A1).

Re claims 1, 8, 18-29 and 31-40: Jiau discloses a compact personal token apparatus 1, comprising: a connection module 1312 (paragraph [0044]); a translation module, which incorporated with a processor module 132; and an input/output module [139, 1341, 1342, 1343, 1344] (figs. 1 & 3A-3C); the translation module moves signals between a USB interface and a wireless interface (paragraphs [0050-0051]); an LCD screen 1341 and LEDs 1342 (fig. 3C); a standard-compliant contact based interface, the contact based interface complying to at least one standard interface selected from the group consisting of USB, IEEE 1394, PCMCIA, Compact Flash, Multi Media, Memory Stick, Smart Media, Secure Digital, mini SD, IBM Micro Drive, and any similar standard interface (paragraph [0044]); a standard-compliant contactless/wireless interface 1311; the contactless/wireless interface 1311 complying to one or more of the following standard interfaces: RFID-contactless interface according to WLAN 812.11 and Bluetooth compatible interface (paragraphs [0047] & [0050]); a flash memory 133 (fig. 3A); wherein: the dual interface chip (processor) inside the personal token can be directly programmed by a software running on the host system using the interface processor without the need for an external contact based dual interface read/write device (paragraph [0052]); wherein: the downloaded information can be used in the real world; wherein: the software is web based, allowing for downloading information from the web directly into the dual interface processor memory thus linking the virtual world to the real world (paragraph [0052]); wherein: the information stored in the personal token via the standard contact based interface is used for personal identification, secure network logon, access control, e-ticketing, e-payment and similar applications using either the standard compliant interface or the RFID-compliant interface (paragraph [0067]).

Claim Rejections - 35 USC § 103

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

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

8. This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

9. Claims 10 and 11 are rejected under 35 U.S.C. 103(a) as being unpatentable over Jiau in view of Weng (US 6983888 B2). The teachings of Jiau have been discussed above.

Re claims 10 and 11: Jiau has been discussed above, but is silent with respect to the translation module moves data or signals from a USB interface to an RFID interface and a wireless interface with storage of data in a flash memory or EEPROM of the processor module, and data can reside temporarily at one of the interfaces; the translation module is incorporated in the processor module so that the personal token apparatus can go directly from USB to wireless without being limited by smart card software architecture limitations; respectively.

Weng teaches a body proper 1 having a receiver 12 and a transmitter 21 (i.e., RF or wireless interface), a flash memory 11, a USB interface control circuit 15, and a monode control switch 13 for switching from USB to wireless, all of which are interconnected; wherein when the high frequency receiver circuit (12) receives transmitted signals, through the monode control switch (13), the firewall (14) is turned on rendering the flash memory (11) to be read-and-writeable by the USB interface control circuit (15) (fig. 3; col. 2, lines 25-36).

It would have been obvious to an artisan of ordinary skill in the art at the time the invention was made to incorporate the teachings of Weng into the system as taught by Jiau due to the fact that such modification would have been an obvious engineering variation, well within the ordinary skill in the art, for intended use (i.e., for transmitting data/signal from RF/wireless interface to USB interface and vise versa), and therefore an obvious expedient.

10. Claims 17, 45 and 52 are rejected under 35 U.S.C. 103(a) as being unpatentable over Margalit et al in view of Jiau. The teachings of Margalit et al and Jiau have been discussed above.

Re claims 17, 45 and 52: Margalit et al has been discussed above but is silent with respect to a contactless interface.

Jiau teaches a communication unit 131 includes wireless connection 1311 (fig. 3B; paragraph [0051]).

It would have been obvious to an artisan of ordinary skill in the art at the time the invention was made to incorporate a wireless connection of Jiau into the system as taught by Margalit et al in order to provide Margalit et al with a universal system wherein the system can be utilized in any type of communications (i.e., contact, contactless, USB, etc.). Furthermore, such modification would provide the user the flexibility in using the system wherein the user does not have to concern about whether or not the system is compatible with a particular communication system that the user intend to use, and therefore an obvious expedient.

11. Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over Jiau in view of Margalit et al. The teachings of Jiau and Margalit et al have been discussed above.

Re claim 30: Jiau has been discussed above but is silent with respect to an interface that is complying to ISO 7810 or a 7816 compliant SIM module.

Margalit et al teaches a personal token apparatus 125 having an interface that is a 7816 compliant SIM module (fig. 2).

It would have been obvious to an artisan of ordinary skill in the art at the time the invention was made to incorporate a 7816 compliant SIM module of Margalit et al into the system as taught by Jiau in order to provide Jiau with a universal system wherein the system can be utilized in any type of communications (i.e., contact, contactless, USB, etc.). Furthermore, such modification would provide the user the flexibility in using the system wherein the user does not have to concern about whether or not the system is compatible with a particular communication system that the user intend to use, and therefore an obvious expedient.

Response to Arguments

12. Applicant's arguments filed 14 November 2005 have been fully considered but they are not persuasive.

13. In response to the Applicant's argument to "a contactless interface", which is not being taught by the cited references to Margalit et al and Jiau (p. 16, lines 26-28; p. 17, line 28), the Examiner respectfully draws the Applicant's attention to claims 5 and 49, where the claims recite "the smart card interface is *selected from the group consisting of…,*" which means *any one* selected from the group (*not all* of the group) can be read into the

claimed limitation. In this case, Margalit teaches an ISO 7816 interface (fig. 2), which is included within the group claimed by the Applicant. Accordingly, the claimed limitation, given the broadest reasonable interpretation, Margalit et al meets the claimed invention (see the rejection above).

14. In response to applicant's argument that the references fail to show certain features of applicant's invention, it is noted that the features upon which applicant relies (i.e., the combination of USB, contactless, wireless and extended memory with flash (p. 24, lines 3-4)) are not recited in the rejected claim(s). Although the claims are interpreted in light of the specification, limitations from the specification are not read into the claims. See *In re Van Geuns*, 988 F.2d 1181, 26 USPQ2d 1057 (Fed. Cir. 1993).

15. In response to the Applicant's argument to "claims 5, 6 and 49 differ from Margalit with respect to the contactless interface…" (p. 25, lines 6-7), the Examiner respectfully draws the Applicant's attention to claims 5 and 49, where the claims recite "the smart card interface is *selected from the group consisting of…*," which means any <u>*one*</u> selected from the group (<u>*not all*</u> of the group) can be read into the claimed limitation. In this case, Margalit teaches an ISO 7816 interface (fig. 2), which is included within the group claimed by the Applicant. Regarding claim 6, Margalit teaches a processor module comprises a dual interface chip (i.e., a USB

interface and an ISO 7816 interface) (fig. 2). Accordingly, the claimed limitation, given the broadest reasonable interpretation, Margalit et al meets the claimed invention (see the rejection above).

16. In response to the Applicant's argument to "claim 8 is novel over Jiau when refereeing to the RF antenna in connection with contactless and wireless technology" (p. 26, lines 8-9), the Examiner respectfully request the Applicant to further review Jiau wherein a wireless connection 1311 providing dual radio modes of PAN (e.g., Bluetooth) plus WLAN (e.g., IEEE 802.11b) (fig. 3B; paragraph [0051]), which has a build-in antenna (claim 3, lines 22+). Accordingly, the claimed limitation, given the broadest reasonable interpretation, Jiau meets the claimed invention (see the rejection above).

17. Applicant's arguments with respect to claims 10 and 11 have been considered but are moot in view of the new ground(s) of rejection.

Newly cited reference to Weng has used in the new ground of rejection to further meet the newly amended limitation of the claimed invention.

18. In response to the Applicant's argument to claim 22 (p. 26, line 13), the Examiner respectfully request the Applicant to further review Jiau wherein the wireless interface complying/providing dual

radio modes of PAN (e.g., Bluetooth) plus WLAN (e.g., IEEE 802.11b) (fig. 3B; paragraph [0051]), which is *one or more* of the standard interfaces recited in the claim 22. Accordingly, the claimed limitation, given the broadest reasonable interpretation, Jiau meets the claimed invention (see the rejection above).

19. In response to the Applicant's argument to "claim 31 describes a dual interface chip…" (p. 26, line 14+), the Examiner respectfully request the Applicant to further review Jiau wherein dual interface chip/processor 132 having a PAN and WLAN wireless interface and a USB interface (see figs. 3A-3B). Accordingly, the claimed limitation, given the broadest reasonable interpretation, Jiau meets the claimed invention (see the rejection above).

Applicant's amendment and remarks have bee carefully studied and considered, but they are not persuasive. Therefore, the Examiner has made this Office Action final.

Conclusion

20. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

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

21. This action is a **final rejection** and is intended to close the prosecution of this application. Applicant's reply under 37 CFR 1.113 to this action is limited either to an appeal to the Board of Patent Appeals and Interferences or to an amendment complying with the requirements set forth below.

If applicant should desire to appeal any rejection made by the examiner, a Notice of Appeal must be filed within the period for reply identifying the rejected claim or claims appealed. The Notice of Appeal must be accompanied by the required appeal fee of $500.

If applicant should desire to file an amendment, entry of a proposed amendment after final rejection cannot be made as a matter of right unless it merely cancels claims or complies with a formal requirement made earlier. Amendments touching the merits of the application which otherwise might not be proper may be admitted upon a showing a good and sufficient reasons why they are necessary and why they were not presented earlier.

A reply under 37 CFR 1.113 to a final rejection must include the appeal from, or cancellation of, each rejected claim. The filing of an amendment after final rejection, whether or not it is entered, does not stop the running of the statutory period for reply to the final rejection unless the examiner holds the claims to be in condition for allowance. Accordingly, if a Notice of Appeal has not been filed properly within the period for reply, or any extension of this period obtained under either 37 CFR 1.136(a) or (b), the application will become abandoned.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Uyen-Chau N. Le whose telephone number is 571-272-2397. The examiner can normally be reached on First Monday 5:30AM-1:30PM and Tues-Fri 5:30AM-3PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Michael G. Lee can be reached on 571-272-2398. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Uyen-Chau N. Le
Primary Examiner
Art Unit 2876

January 17, 2006

substitute forms PTO/SB/08a & PTO/SB/08b		Application Number	**10/990,296**
		Filing Date	**November 16, 2004**
INFORMATION DISCLOSURE STATEMENT BY APPLICANT		First Named Inventor	Dennis J. Ryan
		Art Unit	2876
		Examiner Name	Uyen Chau N. Lee
Sheet 1	OF 3	Practitioner Docket No.	Ryan C-4

U.S. PATENT DOCUMENTS

Exam. Initials	Cite No.	Document Number No. -Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Relevant Pages, Columns, Lines
UL	A	US-3,941,489	03-22-1974	Bryan	
	B	US-4,367,965	01-11-1983	Speitel et al.	
	C	US-5,761,648	06-02-1998	Golden et al.	
	D	US-6,067,235	05-23-2000	Finn et al.	
	E	US 6,085,320	07-04-2000	Kaliski, Jr.	
	F	US 6,148,354	11-14-2000	Ban et al.	
	G	US 6,168,077	01-02-2001	Gray et al.	
	H	US 6,189,098	02-13-2001	Kaliski, Jr.	
	I	US 6,240,184	05-29-2001	Huynh et al.	
	J	US 6,283,658	09-04-2001	Estevez et al.	
	K	US 6,370,603	04-09-2002	Silverman et al.	
	L	US 6,385,677	05-07-2002	Yao	
	M	US 6,505,773	01-14-2003	Palmer et al.	
	N	US 6,543,690	04-08-2003	Leydier et al.	
	O	US 6,567,273	05-20-2003	Liu et al.	
	P	US 6,658,516	12-02-2003	Yao	
	Q	US 6,694,399	02-17-2004	Leydier et al.	
	R	US 6,724,680	04-20-2004	Ng et al.	
	S	US 6,748,541	06-08-2004	Margalit et al.	
	T	US 6,752,321	06-22-2004	Leaming	
	U	US 6,763,399	07-13-2004	Margalit et al.	
	V	US 6,772,956	08-10-2004	Leaming	
	W	US 6,798,169	09-28-2004	Stratmann et al.	
	X	US 6,801,956	10-05-2004	Feuser et al.	
	Y	US 6,848,045	01-25-2005	Long et al.	
	Z	US 6,876,420	04-05-2005	Hong et al.	
	AA	US 6,879,597	04-12-2005	Tordera et al.	
	BB	US 2001 0043702	11-22-2001	Elteto et al.	
	CC	US 2001 0054148	12-20-2001	Hoornaert	
	DD	US 2002 0011516	01-31-2002	Lee	
	EE	US 2003 0000267	01-02-2003	Jacob et al.	
	FF	US 2003 0028797	02-06-2003	Long et al.	
	GG	US 2003 0087601	05-08-2003	Agam et al.	
	HH	US 2003 0102380	06-05-2003	Spencer	
↓	II	US 2003 0236821	12-25-2003	Jiau	

substitute forms PTO/SB/08a & PTO/SB/08b	Application Number	**10/990,296**
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Filing Date	**November 16, 2004**
	First Named Inventor	Dennis J. Ryan
	Art Unit	2876
	Examiner Name	Uyen Chau N. Le
Sheet 2 OF 3	Practitioner Docket No.	Ryan C-4

FOREIGN PATENT DOCUMENTS

Exam. Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Doc.	Relevant Pages, Columns, Lines	T
	f1	DE19631050	02-05-1998	Bergler et al.	Drawings	
	f2	HK 1063994				T
	f3	HK 1063995				T
	f4	JP2004246720	09-02-2004		Drawings	
	f5	WO99 052051	10-14-1999	International Business Machines		T
	f6	WO99 038062	07-29-1999	Kobil Computer GMBH	Abs.(Engl), Dwg.	
	f7	WO00 036252	06-22-2000	Jacob	Abs.(Engl), Dwg.	
	f8	WO00 042491	07-20-2000	Rainbow Technologies, Inc.		T
	f9	WO00 065180	11-02-2000	Muller et al.	Abs.(Engl), Dwg.	
	f10	WO00 075755	12-14-2000	Eutron Infosecurities		T
	f11	WO01 014179	03-01-2001	Wittwer et al.	Abs.(Engl), Dwg.	
	f12	WO01 038673	03-31-2001	Wittwer et al.	Abs.(Engl), Dwg.	
	f13	WO01 039102	11-02-2001	Muller et al.		T
	f14	WO01 048339	07-05-2001	Jacob et al.	Abs.(Engl), Dwg.	
	f15	WO01 048342	07-05-2001	Jacob et al.	Abs.(Engl), Dwg.	
	f16	WO01 061692	08-23-2001	Trek Technology		T
	f17	WO01 088693	11-22-2001	Seysen	Abs.(Engl), Dwg.	
	f18	WO01 096990	12-20-2001	Rainbow Technologies, Inc.		T
	f19	WO03 014887	02-20-2003	Activcard Ireland		T
	f20	WO03 034189	04-23-2003	Activcard Ireland		T
	f21	WO04 002058	12-31-2003	Gemplus	Abs.(Engl), Dwg.	
	f22	WO04 081706	09-23-2004	Digisafe Ltd.		T
	f23	WO04 081769	09-24-2004	Axalto SA		T

NON PATENT LITERATURE DOCUMENTS

Exam. Initials	Cite No.	Name of author (ALL-CAPS), title of article, title of item, date, pages, vol-issue #, publisher, city and/or country where published.	T
	1	*ACR38CT Contactless SIM Tracker Technical Specification*, Advanced Card Systems Ltd., Hong Kong.	T
	2	*ACR38DT Dual Key Technical Specifications, Version 1.3*, September 2004, Advanced Card Systems Ltd., Hong Kong.	T
	3	*Dallas Semiconductor DS1490F 2-in-1 Fob*, Dallas Semiconductor, Dallas TX.	T

substitute forms PTO/SB/08a & PTO/SB/08b **INFORMATION DISCLOSURE STATEMENT BY APPLICANT**	Application Number	**10/990,296**
	Filing Date	**November 16, 2004**
	First Named Inventor	Dennis J. Ryan
	Art Unit	2876
	Examiner Name	Uyen Chau N. Le~~e~~
Sheet 3 OF 3	Practitioner Docket No.	Ryan C-4

NON PATENT LITERATURE DOCUMENTS

Exam. Initials	Cite No.	Name of author (ALL-CAPS), title of article, title of item, date, pages, vol-issue #, publisher, city and/or country where published.	T
	4	*Dallas Semiconductor DS9490-DS9490R USB to 1-Wire/iButton Adaptor*, Maxim I-C, Sunnyvale CA.	T
	5	HARA, YOSHIKO, *Matsushita blends FERAM technology with smart cards*, October 1, 2004, CMP Media, Manhasset NY.	T
	6	*Japan's Matsushita developing memory cards with smart chip function*, October 1, 2004, Mercury News, San Jose CA.	T
	7	*OTi-6828 Flash Disk Controller*, Ours Technology Inc., Taiwan.	T
	8	*Panasonic Develops RFID smartSD Card*, October 4, 2004, Palminfocenter.com, Sunnyvale CA.	T
	9	*Panasonic Develops Industry's First SD Memory Card with Contacless Smart Card Capabilities*, October 1, 2004, The Japan Corporate News Network, Tokyo.	T
	10	ROJAS, PETER, *Panasonic's Smart SD adds RFID to the mix*, October 4, 2004, Engadget LLC, New York NY.	T
	11	*Delivering ultimate security, high performance and ultra low power consumption, SmartMX is now in volume supply*, November 18-20, 2003, Cartes 2003, aris Nort Villepinte, France	T
	12	BALABAN, DAN, *Digital Rights pits SIMS against Flash Cards, Card Technology*, November 2004, pp 24-30, Card Technology, Chicago IL.	T
	13	*P5CT072 Secure Dual Interface PKI Smart Card Controller, Rev. 1.3*, October 2004, Koninklijke Philips Electronics, The Netherlands	T
	14	*Vodafone KK Develops Contactless Smart Card Mobile Handset*, May 6, 2004, HiTEK Magazine, Dubai	T
	15	*SmartSD Card Structure*	T

Examiner Signature

1/17/06
Date Considered

Notice of References Cited	Application/Control No. 10/990,296	Applicant(s)/Patent Under Reexamination RYAN ET AL.	
	Examiner Uyen-Chau N. Le	Art Unit 2876	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,983,888 B2	01-2006	Weng, Cheng-Fu	235/492
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

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

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

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

Index of Claims

	Application/Control No. 10/990,296	**Applicant(s)/Patent under Reexamination** RYAN ET AL.
	Examiner Uyen-Chau N. Le	**Art Unit** 2876

√	**Rejected**	**–**	**(Through numeral) Cancelled**	**N**	**Non-Elected**	**A**	**Appeal**
=	**Allowed**	**÷**	**Restricted**	**I**	**Interference**	**O**	**Objected**

Claim		Date								
Final	Original	1/17/06								
	1	√								
	2	│								
	3	│								
	4	│								
	5	│								
	6	│								
	7	│								
	8	│								
	9	│								
	10	│								
	11	│								
	12	│								
	13	│								
	14	│								
	15	│								
	16	│								
	17	│								
	18	│								
	19	│								
	20	│								
	21	│								
	22	│								
	23	│								
	24	│								
	25	│								
	26	│								
	27	│								
	28	│								
	29	│								
	30	│								
	31	│								
	32	│								
	33	│								
	34	│								
	35	│								
	36	│								
	37	│								
	38	│								
	39	│								
	40	│								
	41	│								
	42	│								
	43	│								
	44	│								
	45	│								
	46	│								
	47	│								
	48	│								
	49	│								
	50	√								

Claim		Date								
Final	Original	1/17/06								
	51	√								
	52	√								
	53									
	54									
	55									
	56									
	57									
	58									
	59									
	60									
	61									
	62									
	63									
	64									
	65									
	66									
	67									
	68									
	69									
	70									
	71									
	72									
	73									
	74									
	75									
	76									
	77									
	78									
	79									
	80									
	81									
	82									
	83									
	84									
	85									
	86									
	87									
	88									
	89									
	90									
	91									
	92									
	93									
	94									
	95									
	96									
	97									
	98									
	99									
	100									

Claim		Date								
Final	Original									
	101									
	102									
	103									
	104									
	105									
	106									
	107									
	108									
	109									
	110									
	111									
	112									
	113									
	114									
	115									
	116									
	117									
	118									
	119									
	120									
	121									
	122									
	123									
	124									
	125									
	126									
	127									
	128									
	129									
	130									
	131									
	132									
	133									
	134									
	135									
	136									
	137									
	138									
	139									
	140									
	141									
	142									
	143									
	144									
	145									
	146									
	147									
	148									
	149									
	150									

Search Notes	Application/Control No. 10/990,296	Applicant(s)/Patent under Reexamination RYAN ET AL.	
	Examiner Uyen-Chau N. Le	Art Unit 2876	

SEARCHED

Class	Subclass	Date	Examiner
SEARCH	UPDATED	1/17/2006	UCL

INTERFERENCE SEARCHED

Class	Subclass	Date	Examiner

SEARCH NOTES (INCLUDING SEARCH STRATEGY)

	DATE	EXMR
Text search only -- see search history printout	1/17/2006	UCL
EAST (US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB)	1/17/2006	UCL

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	33	("20010043702"|"20010054148"|"20020011516"|"20030000267"|"20030028797"|"20030102380"|"20030236821"|"3941489"|"4367965"|"5761648"|"6067235"|"6085320"|"6148354"|"6168077"|"6189098"|"6240184"|"6283658"|"6370603"|"6385677"|"6505773"|"6543690"|"6567273"|"6658516"|"6694399"|"6724680"|"6752321"|"6763399"|"6772956"|"6798169"|"6801956"|"6848045"|"6876420"|"6879597").PN.	US-PGPUB; USPAT	OR	ON	2006/01/17 14:32
S1	2181	data near30 temporary near30 interfac$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/01/17 09:27
S2	1585	(data signal) near30 usb near30 (wire$1less rf$2)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/01/17 10:16
S3	0	S1 same S2	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/01/17 09:28
S4	12	S1 and S2	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/01/17 10:02
S5	292	router same wireless same usb	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/01/17 10:05
S6	7490	dual near10 interface	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/01/17 10:03
S7	0	S5 same S6	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/01/17 10:03

S8	20	S5 and S6	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/01/17 10:04
S9	53	router near30 wireless near30 usb	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/01/17 10:06
S10	1699	(data signal) near30 usb near30 (wire$1less rf$2 antenna)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/01/17 10:17
S11	161	S10 and "235"/$.ccls.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/01/17 10:17
S12	15	("20020192009" | "20030043111" | "20040064728" | "20040080989" | "20050083315" | "5952641" | "6088450" | "6446862" | "6504480" | "6522534" | "6561421" | "6594154" | "6763315" | "6763410" | "6837422").PN. OR ("6983888"). URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2006/01/17 10:30
S13	2	"20030236821"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/01/17 11:35

UNITED STATES PATENT AND TRADEMARK OFFICE

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

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/990,296	11/16/2004	Dennis J. Ryan	Ryan C-4	2050

37053 7590 04/17/2006

D.A. STAUFFER PATENT SERVICES LLC
1006 MONTFORD ROAD
CLEVLAND HTS., OH 44121-2016

EXAMINER	
LE, UYEN CHAU N	
ART UNIT	**PAPER NUMBER**
2876	

DATE MAILED: 04/17/2006

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

PTO-90C (Rev. 10/03)

R

Interview Summary	Application No.	Applicant(s)	
	10/990,296	RYAN ET AL.	
	Examiner	**Art Unit**	
	Uyen-Chau N. Le	2876	

All participants (applicant, applicant's representative, PTO personnel):

(1) *Uyen-Chau N. Le*. (3)_____.

(2) *Gerald F. Linden (Reg. 30,282)*. (4)_____.

Date of Interview: *06 April 2006*.

Type: a)☒ Telephonic b)□ Video Conference
c)□ Personal [copy given to: 1)□ applicant 2)□ applicant's representative]

Exhibit shown or demonstration conducted: d)□ Yes e)□ No.
If Yes, brief description: _____.

Claim(s) discussed: _____.

Identification of prior art discussed: _____.

Agreement with respect to the claims f)□ was reached. g)☒ was not reached. h)□ N/A.

Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: *Mr. Linden explained the differences between contactless and wireless, and proposed new amended claims. Upon receiving a formal amendment and response, further search and consideration will be made*.

(A fuller description, if necessary, and a copy of the amendments which the examiner agreed would render the claims allowable, if available, must be attached. Also, where no copy of the amendments that would render the claims allowable is available, a summary thereof must be attached.)

THE FORMAL WRITTEN REPLY TO THE LAST OFFICE ACTION MUST INCLUDE THE SUBSTANCE OF THE INTERVIEW. (See MPEP Section 713.04). If a reply to the last Office action has already been filed, APPLICANT IS GIVEN A NON-EXTENDABLE PERIOD OF THE LONGER OF ONE MONTH OR THIRTY DAYS FROM THIS INTERVIEW DATE, OR THE MAILING DATE OF THIS INTERVIEW SUMMARY FORM, WHICHEVER IS LATER, TO FILE A STATEMENT OF THE SUBSTANCE OF THE INTERVIEW. See Summary of Record of Interview requirements on reverse side or on attached sheet.

Uchaule

UYEN-CHAU N. LE
PRIMARY EXAMINER

Examiner Note: You must sign this form unless it is an Attachment to a signed Office action.

____
Examiner's signature, if required

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)
In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:

- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:

1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner, .
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Inventor(s): Ryan, et al. Confirmation Number: 2050

Title: MULTI-INTERFACE COMPACT PERSONAL TOKEN APPARATUS AND METHODS OF USE

Serial Number: 10/990,296 Publication No. 20050109841

Filing Date: 11/16/2004 Publication Date 5/26/2005

Docket No.: Ryan C-4

Examiner: Le, Uyen Chau N. Art Unit: 2876
phone: 571-272-2397

April 25, 2006

COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, VA 22313-1450

RCE with Amendment and IDS

This document is a submission for a Request for Continued Examination (RCE) under 37 CFR 1.114 in the above-referenced patent application, currently under final rejection. This submission includes amendments detailed hereinbelow.

Amendments to the Specification begin on page 2.

Amendments to the Claims begin on page 9.

Remarks begin on page 19.

The present submission also includes a new Information Disclosure Statement (IDS) along with copies of foreign patents and documents. According to 37 CFR 1.97(b)(4) there is no fee required for an IDS submitted along with an RCE. It may be noted that an IDS was previously submitted wherein the foreign patent/document copies were mistakenly submitted on a CDROM and therefore were not considered entered. The presently submitted IDS includes one additional US Patent reference compared to the previous IDS, therefor the present IDS supercedes the previously submitted one.

IN THE SPECIFICATION

in the previous amendment, the following amendment was made:
At page 1, lines 4-5 (entire paragraph)
This is a non-provisional filing based on USSN 60/520,698 filed 11/17/2003 by Ryan, Comiskey, ~~and~~ Knapich and Finn.

Please enter the following amendments in the specification (and abstract).
References are made to page and line numbers and/or to numbered paragraphs of the published patent application.

in the paragraph [0072], at page 13, beginning on line 17.

IEEE ~~812.11~~ 802.11 The IEEE standard for wireless Local Area Networks (LANs). It uses three different physical layers, 802.11a, 802.11b and 802.11g.

in the paragraphs [0089-0090], at page 16, beginning on line 6.

NFC Short for "Near Field Communication". NFC is a ~~wireless~~ contactless connectivity technology that enables short-range communication between electronic devices. If two devices are held close together (for example, a mobile phone and a personal digital assistant), NFC interfaces establish a peer-to-peer protocol, and information such as phone book details can be passed freely between them. NFC devices can be linked to contactless smart cards, and can operate like a contactless smart card, even when powered down. This means that a mobile phone can operate like a transportation card, and enable fare payment and access to the subway.

NFC is an open platform technology standardized in ECMA (European Computer Manufacturers Association) 340 as well as ETSI (European Telecommunications Standards Institute) TS 102 190 V1.1.1 and ISO/IEC 18092. These standards specify the modulation schemes, coding, transfer speeds, and frame format of the RF interface of NFC devices, as well as initialisation schemes and conditions required for data collision-control during initialisation – for both passive and active modes.

in the paragraph [0124], at page 22, beginning on line 11.

The invention is generally a compact personal token apparatus which can be plugged into a personal computer and interfaced with the virtual world of the Internet. The apparatus (or, as will be evident, a portion of a modular apparatus) can then be removed from the personal computer and used to conduct real world transactions. The compact personal token apparatus is suitably in the general form of a fob, resembling a USB memory fob. The compact personal token apparatus comprises a contactless ~~wireless~~ interface and may also comprise a wireless interface.

in the paragraph [0130], at page 23, beginning on line 16.

According to a feature of the invention, the compact personal token apparatus (or equivalent) may remain in the apparatus capable of interacting with the personal token (e.g., cell phone, PDA), when the personal token device communicates contactlessly ~~(e.g., wirelessly)~~ in the real world. It does not necessarily have to be removed from the host device.

in the paragraph [0134], at page 24, beginning on line 20.

The apparatus may further comprise a standard–compliant contactless ~~/wireless interface; the contactless/wireless~~ interface complying to one or more of the following standard interfaces: RFID-contactless interface according to ISO 14443 and ISO 15693 as well as similar interfaces, and a wireless interface complying to one or more of the following standard interfaces: Bluetooth compatible interface, WLAN ~~812.11~~ 802.11, UWB, and any similar interface.

in the paragraph [0136], at page 25, beginning on line 5.

The apparatus may further comprise a standard-compliant interface releaseably coupleable to a host processing device, this being under the command of an operating system; an interface module providing translation of standard-compliant contact based interface messages via a memory chip to Bluetooth /WLAN ~~812.11~~ 802.11device compatible compliant messages, and providing the translation of Bluetooth /WLAN ~~812.11~~ 802.11device compliant messages via a memory chip to standard-compliant contact based interface messages; a Bluetooth /WLAN ~~812.11~~ 802.11device having a Bluetooth/WLAN ~~812.11~~ 802.11compliant interface communicating through the interface module with the host processing device via a memory chip; the same Bluetooth /WLAN ~~812.11~~ 802.11device communicating through its Bluetooth /WLAN ~~812.11~~ 802.11compatible interface.

in the paragraph [0139], at page 26, beginning on line 1.

The contactless and/or wireless module may be releaseably coupleable from the interface module.

in the paragraph [0145], at page 26, beginning on line 21.

The apparatus may further comprise a processor module, preparing messages to be sent by the contactless and/or wireless interfaces [[of]] and interpreting messages received via the interface(s).

in the paragraph [0148], at page 27, beginning on line 3.

According to the invention, a method of interacting contactlessly and/or wirelessly comprises: providing a device; interfacing the device with a an Internet-capable appliance; and providing a smart card interface in the device.

in the paragraph [0151], at page 27, beginning on line 12.

The "smart fob" is capable of loading and storing information from the Internet, via a PC or other Internet capable device to its memory and then using the stored information via its ~~wireless~~ contactless interface in the real world. The "smart fob" is also capable of exchanging information with a conventional smart card.

in the paragraph [0166], at page 29, beginning on line 6 .

This invention relates generally to devices, technology and applications for downloading and interacting with data and value from one "world" such as the virtual world of the Internet and, with the device, interacting, typically ~~wirelessly~~ contactlessly, with another "world" such as the physical world of banking, stores (point of sale), physical access control, and the like.

in the paragraph [0167], at page 29, beginning on line 10.

Generally, this is done using a device running software and interacting with an Internet capable apparatus such as a personal computer (PC), a personal digital assistant (PDA) or a handset (Internet capable cell phone). In many embodiments, the device interacts with the physical world using a standard ~~wireless~~ contactless smart card interface, such as ISO 14443 or 15693. In some embodiments, the device plugs into a PC using a standard contact interface, such as USB. Several embodiments and several applications applicable to various ones of the embodiments are discussed.

in the paragraph [0168], at page 29, beginning on line 17.

In an embodiment, the device is embodied in the form of a compact personal token apparatus, resembling a conventional USB memory fob (size, shape, form) which can be plugged into an apparatus such as a personal computer (PC) and interfaced with the virtual world of the Internet. The device is capable of loading and storing information from the Internet, via the PC to its flash memory (memory that can be erased and reprogrammed in blocks) or EEPROM and then using the stored information or value via its ~~wireless~~ contactless interface in the real world. Similarly, the device is capable of implementing an auto-run application, when inserted into a personal computer (PC) connected to the Internet, and information exchanged and stored can be accessed in the real world application via its ~~wireless~~ contactless interface. The memory space required for the auto-run application can reside completely in the device or only partially in the device. Additional memory space to complete the application can be located on the server of the ISP, trusted third party or host server. The apparatus is also capable of exchanging information with other devices having compatible interfaces.

in the paragraph [0180], at page 31, beginning on line 22.

Alternatively, the translation module can go from USB to ISO 14443 or 15693 (~~wireless~~ contactless interfaces). The latter is shown in FIG. 1B, and is described hereinbelow. In going directly from USB to ~~wireless~~ contactless, the device is not limited by the smart card software architecture (ISO 7816) limitations. The translation module in this case is a processor device, that will handle the data processing from USB to ~~wireless~~ contactless.

in the paragraph [0181], at page 32, beginning on line 3.

The processor module 106 is for controlling operation of the compact personal token apparatus ("device") of the present invention and is preferably capable of operating as a dual-interface (DI) chip. For example, Mifare ProX, Infineon 66 series, etc. The dual interface chip is available from various vendors (e.g., Philips, Infineon, ST Microelectronic), and is capable of interfacing from ISO 7816 (contact interface) to either or both of ISO 14443 and 15693 (~~wireless~~ contactless interfaces).

in the paragraph [0184], at page 32, beginning on line 17.

As mentioned above, alternatively, the translation module can go from USB to ISO 14443 or 15693. In other words, directly from USB to ~~wireless~~ contactless.

in the paragraph [0192], at page 33, beginning on line 7.

Unlike the previous embodiment, in this embodiment the translation module 124 goes from USB to a ~~wireless~~ contactless interface. Therefore, the processor module 126 does not need to be a dual interface (DI) chip. Rather, the processor module 126 could simply comprise a USB interface on one side and a ~~wireless~~ contactless interface on the other. The memory of the processor could be used as temporary storage and the processor could handle the data encoding as well.

in the paragraph [0203], at page 34, beginning on line 21.

Figure 2B illustrates another exemplary embodiment 220 of the smart fob, again in the general form of a USB memory fob. But in this case, the smart fob has a first physical module 222 (left, as viewed) which contains the ~~input~~ connection module (e.g., 102, USB plug, cf. 212) and translation module (e.g., 104), and a second physical module 224 (right, as viewed) which contains the processor module (e.g., 106, dual-interface chip) and output module (e.g., 108, RF antenna and modulator). The two modules 222 and 224 can plug together and be taken apart from one another. In this manner, after interacting with the "virtual world" on his computer, the user can separate the two modules 222 and 224 and carry just the second module, for conducting "real world" transactions. The second module 224, comprising processor and output module, is sufficient for conducting real world, ~~wireless~~ contactless transactions, in the manner of a smart card. In other words, the smart fob can emulate a smart card.

in the paragraph [0212], at page 36, beginning on line 19.

- an input module 408 which, unlike other embodiments, need not perform wireless or contactless functions, but rather is socket (or plug), such as RJ-45, for connecting to a telephone line (or the like) supporting a DSL (or the like) connection to the Internet.

in the paragraph [0223], at page 37, beginning on line 14.

In use, for example, the user plugs the smart fob into his PC, or other Internet capable device (appliance), connects to the Internet, and interacts with a service or content provider to upload and/or download information. For example, downloading a ticket. Then, the user takes the smart fob to the event where it connects wirelessly or contactlessly with a reader at the venue to allow entrance and stamp the ticket (e.g., set a flag indicating that the ticket was used).

in the paragraph [0235], at page 39, beginning on line 22.

In use, for example, the user plugs the smart fob device into a PC, connects to the Internet, and interacts with a service or content provider to upload and/or download information. For example, the user can download an event ticket, take the device to the venue, just wave the device in close proximity to a turnstile equipped with a ~~wireless~~ contactless reader at the entrance, and access is granted without having to stand in line.

in the paragraph [0240], at page 40, beginning on line 14.

As mentioned above, the smart fob (device) is capable of implementing an auto-run application, when inserted into a personal computer (PC) connected to the Internet, and information exchanged and stored can be accessed in the real world application via its wireless and/or contactless interface.

in the paragraph [0247], at page 41, beginning on line 19.

Therefore, the smart fob can be viewed as a marketing platform that encapsulates auto-run application software for a specific application, a USB apparatus for memory management and radio frequency identification, mass storage capability, a secure server for authentication and filtering as well as a wireless and/or contactless interface, to provide a myriad of solutions addressing marketing, e-commerce, business productivity, IT (information technology), consumer, communication, content, security and mobility issues.

in the paragraph [0248], at page 42, beginning on line 1.

The smart fob can be used as a payment device for retail purchase & loyalty with the Internet feature allowing users to download value, coupons, tickets, entertainment content, etc. The smart fob can be personalised like a conventional credit/debit card for electronic payment and the wireless and/or contactless interface feature can be used for photo identification, to download transit & event tickets, to receive complimentary coupons, loyalty points, gift certificates and messages, for vending and to redeem coupons. In addition the smart fob eliminates the need to tender with cash.

at page 67, (abstract)

A compact personal token apparatus (100,120,140,200,220,300,320,500), resembling a conventional USB memory fob in size, shape, and form which can be plugged into a PC and interfaced with the virtual world of the Internet. The apparatus is capable of loading and storing information from the Internet, via the PC to its flash memory (410) or EEPROM and then using the stored information or value via its ~~wireless~~ contactless interface (108,128,148,508) in the real world. The apparatus is capable of implementing an auto-run application, when inserted into a personal computer. The apparatus is capable of exchanging information with other devices having compatible interfaces. The apparatus can also function as a firewall (400) when plugged between an Internet connection and a PC.

IN THE CLAIMS

Please add or amend the claims to read as follows, and cancel without prejudice or disclaimer to resubmission in a divisional or continuation application claims indicated as cancelled:

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

Listing of Claims:

1. (currently amended) A compact personal token apparatus, comprising:

a connection module;

a translation module;

a processor module; and

an input/output module;

wherein:

the connection module is for interfacing the personal token apparatus with an Internet-capable appliance; and

the translation module moves signals between the connection module and a contactless interface.

2. (currently amended) The compact personal token apparatus of claim 1, wherein:

~~the connection module is for interfacing the personal token apparatus with an Internet-capable appliance; and~~

the Internet-capable appliance comprises a device selected from the group consisting of personal computer (PC), laptop, PDA, MP3 player cellphone, and similar Internet-capable devices; and

the interface with the Internet-capable applicance is selected from the group consisting of USB, FireWire, IR, Bluetooth, standard serial port, WLAN, and similar interfaces capable of interfacing with the Internet-capable appliance.

3. (currently amended) The compact personal token apparatus of claim 1, wherein:

the interface with the Internet-capable appliance comprises a USB connection

~~the connection module is for interfacing the personal token apparatus with an Internet-capable appliance; and~~

~~the Internet-capable appliance comprises a device selected from the group consisting of personal computer (PC), laptop, PDA, MP3 player and cellphone~~.

4. (currently amended) The compact personal token apparatus of claim 1, wherein:
~~the translation module moves signals between a USB interface and~~ the contactless interface comprises a smart card interface.

5. (currently amended) The compact personal token apparatus of claim 4, wherein:
the smart card interface is selected from the group consisting of ~~ISO 7816, ISO 14443 (RFID-contactless interface), and ISO 15693 (RFID-contactless interface)~~ ISO 14443, ISO 15693, NFC and similar contactless interfaces .

6. (original) The compact personal token apparatus of claim 1, wherein:
the processor module comprises a dual interface (DI) chip.

7. (original) The compact personal token apparatus of claim 1, wherein:
the processor module incorporates the translation module.

8. (original) The compact personal token apparatus of claim 1, wherein:
the output module comprises an RF antenna and a modulator.

9. (original) The compact personal token apparatus of claim 1, further comprising:
flash memory.

10. (previously presented) The compact personal token apparatus of claim 1, wherein:
the translation module moves data or signals from a USB interface to an RFID interface and a wireless interface with storage of data in a flash memory or EEPROM of the processor module (dual interface chip), and data can reside temporarily at one of the interfaces.

11. (currently amended) The compact personal token apparatus of claim 1, wherein:

the translation module is incorporated in the processor module so that the personal token apparatus can go directly from USB to ~~wireless (including RFID)~~ contactless without being limited by smart card software architecture limitations.

12. (previously presented) The compact personal token apparatus of claim 1, wherein:

the connection, translation, processor and input/output modules are embodied in a form of an apparatus having a general physical configuration of a conventional USB memory fob.

13. (currently amended) The compact personal token apparatus of claim 12, wherein the fob comprises;

a first physical module containing the ~~input~~ connection module and the translation module; and

a second physical module containing the processor module and the output module.

14. (original) The compact personal token apparatus of claim 1, wherein:

the output module comprises contacts for interfacing with a smart card.

15. (previously presented) The compact personal token apparatus of claim 1, wherein:

the fob is configured for interfacing with the Internet and emulating a smart card.

16. (currently amended) The compact personal token apparatus of claim 1, wherein:

the connection module is for interfacing the personal token apparatus with an Internet-capable appliance; ~~and further comprising:~~

~~an input module is for connecting to the Internet; and~~

the personal token apparatus incorporates firewall functionality to protect the Internet-capable appliance.

17. (original) The compact personal token apparatus of claim 1, further comprising:

interfaces for ISO contact, contactless, USB and DSL.

18. (original) The compact personal token apparatus of claim 1, further comprising:

an LCD screen.

19. (original) The compact personal token apparatus of claim 1, further comprising:
at least one switch.

20. (original) The compact personal token apparatus of claim 1, further comprising:
at least one LED.

21. (currently amended) The compact personal token apparatus of claim 1, further comprising:
~~A compact personal token apparatus comprising:~~

a standard–compliant contact based interface, the contact based interface complying to at least one standard interface selected from the group consisting of USB, IEEE 1394, PCMCIA, Compact Flash, Multi Media, Memory Stick, Smart Media, Secure Digital, mini SD, IBM Micro Drive, and any similar standard interface.

22. (currently amended) The compact personal token apparatus of claim 1, further comprising:
~~The compact personal token apparatus of claim 21, further comprising:~~

a standard–compliant ~~contactless/~~wireless interface selected from the group consisting of ~~; the contactless/wireless interface complying to one or more of the following standard interfaces: wireless interface, RFID-contactless interface according to ISO 14443 and ISO 15693 as well as similar wireless interfaces,~~ Bluetooth compatible interface, WLAN ~~812.11~~ 802.11, UWB, and any similar interface.

23. (currently amended) The compact personal token apparatus of claim 22, further comprising:

a standard-compliant interface releaseably coupleable to a host processing device, this being under a command of an operating system;

an interface module providing translation of standard-compliant contact based interface messages via a memory chip to Bluetooth /WLAN ~~812.11~~ 802.11device compatible compliant messages, and providing the translation of Bluetooth /WLAN ~~812.11~~ 802.11device compliant messages via a memory chip to standard-compliant contact based interface messages; and

a Bluetooth /WLAN ~~812.11~~ 802.11device having a Bluetooth/WLAN ~~812.11~~ 802.11compliant interface communicating through the interface module with the host processing device via a memory chip; the same Bluetooth /WLAN ~~812.11~~ 802.11device communicating through ~~its~~ a Bluetooth /WLAN ~~812.11~~ 802.11compatible interface.

24. (previously presented) The compact personal token apparatus of claim 23, wherein:
    the contactless / wireless interface is releaseably coupleable from the interface module.

25. (original) The compact personal token apparatus of claim 22, further comprising:
    a processor module; and
    additional memory selected from the group consisting of flash memory and EEPROM device powered and addressed by the processor module;
    wherein the additional memory can be used for user authentication and to run applications.

26. (original) The compact personal token apparatus of claim 22, further comprising:
    a standard–compliant smart card contact interface complying to ISO 7816, or any similar interface.

27. (previously presented) The compact personal token apparatus of claim 22, further comprising:
    a processor module, preparing messages to be sent by the contactless/wireless interface and interpreting messages received via the interface.

28. (previously presented) The compact personal token apparatus of claim 21, further comprising:
    a standard-compliant interface releaseably coupleable to a host processing device, this being under a command of an operating system;
    an interface module providing translation of standard-compliant contact based interface messages to ISO 7816 compliant messages and providing the translation of ISO 7816 compliant messages to standard-compliant contact based interface messages;
    a dual interface processor having an ISO7816 compliant interface communicating through the interface module with the host processing device, the dual interface processor communicating through an RFID-contactless interface and connected to an inductive antenna.

29. (previously presented) The compact personal token apparatus of claim 28, wherein:

the contactless / wireless interface is releaseably coupleable from the interface module.

30. (previously presented) The compact personal token apparatus of claim 28, wherein:

the dual interface processor is mounted in a dual interface card complying to ISO 7810 or a 7816 compliant SIM module and connected norms;

the compact personal token apparatus provides physical contacts for the dual interface card, or a 7816 compliant form factor; and

when connected, the dual interface or SIM card can communicate with the host processing device through the interface module inside the personal token apparatus and, once the communication is done, the card can be released from the personal token apparatus and can be used then in the real world.

31. (previously presented) The compact personal token apparatus of claim 28, wherein:

the dual interface chip (processor) inside the personal token apparatus can be directly programmed by a software running on the host system using the interface processor without the need for an external contact based dual interface read/write device.

32. (previously presented) The compact personal token apparatus of claim 31, wherein:

the software is web based, allowing for downloading information from the web directly into the dual interface processor memory, thus linking the virtual world to the real world.

33. (previously presented) The compact personal token apparatus of claim 32, wherein:

the downloaded information can be used in the real world by using the contactless RFID interface.

34. (canceled)

35. (previously presented) The compact personal token apparatus of claim 33, wherein:

the information stored in the personal token apparatus via the standard contact based interface is used for personal identification, secure network logon, access control, e-ticketing, e-payment and similar applications using either the standard compliant interface or the RFID-compliant interface.

36. (previously presented) The compact personal token apparatus of claim 33, wherein:

information received through the RFID- interface can be stored in the memory of the personal token apparatus and can then be provided to the host processing device via the standard interface, thus allowing a complete information exchange between the virtual world and the real world.

37. (previously presented) The compact personal token apparatus of claim 31, wherein:

the information stored in the personal token apparatus via the standard contact based interface is used for personal identification, secure network logon, access control, e-ticketing, e-payment and similar applications using either the standard compliant interface or the RFID-compliant interface.

38. (previously presented) The compact personal token apparatus of claim 31, wherein:

information received through the RFID- interface can be stored in the memory of the personal token apparatus and can then be provided to the host processing device via the standard interface, thus allowing a complete information exchange between the virtual world and the real world.

39. (original) The compact personal token apparatus of claim 31, further comprising:

additional memory selected from the group consisting of flash memory and EEPROM device powered and addressed by the processor module;

wherein the additional memory can be used for user authentication and to run applications.

40. (currently amended) The compact personal token apparatus of claim 21, further comprising:

a standard-compliant interface releaseably coupleable to a host processing device, this being under a command of an operating system;

an interface module providing translation of standard-compliant contact based interface messages via a memory chip to Bluetooth /WLAN ~~812.11~~ 802.11 device compatible compliant messages, and providing the translation of Bluetooth /WLAN ~~812.11~~ 802.11 device compliant messages via a memory chip to standard-compliant contact based interface messages; and

a Bluetooth /WLAN ~~812.11~~ 802.11 device having a Bluetooth/WLAN ~~812.11~~ 802.11 compliant interface communicating through the interface module with the host processing device via a memory chip; the same Bluetooth /WLAN ~~812.11~~ 802.11 device communicating through its Bluetooth /WLAN ~~812.11~~ 802.11 compatible interface.

41. (original) The compact personal token apparatus of claim 21, further comprising:

a processor module; and

additional memory selected from the group consisting of flash memory and EEPROM device powered and addressed by the processor module;

wherein the additional memory can be used for user authentication and to run applications.

42. (original) The compact personal token apparatus of claim 21, further comprising:

a standard–compliant smart card contact interface complying to ISO 7816, or any similar interface.

43. (previously presented) The compact personal token apparatus of claim 21, further comprising:

a connection module, connecting the personal token apparatus to a host device including PC, PDA, smart cellular phone or similar device, either directly or with the help of a standard reader device such as a memory card reader.

44. (previously presented) The compact personal token apparatus of claim 21, further comprising:

a standard-compliant interface releaseably coupleable to a host processing device, this being under a command of an operating system; and

a translation module, translating messages incoming from the contact based interface, and translating messages to the host device from the personal token apparatus.

45. (previously presented) The compact personal token apparatus of claim 21, further comprising:

a triple interface processor including contact, contactless, USB.

46. (currently amended) Method of interacting wirelessly, comprising:

providing a device;

interfacing the device with an Internet-capable appliance; and

providing a smart card interface in the device selected from the group consisting of ISO 14443 and ISO 15693.

47. (original) Method, according to claim 46, wherein:

the interface with the Internet-capable appliance is selected from the group consisting of USB, FireWire, IR, Bluetooth, standard serial port, WLAN.

48. (original) Method, according to claim 46, wherein:

the Internet-capable appliance comprises a device selected from the group consisting of personal computer (PC), laptop, PDA, MP3 player and cell phone.

49. (canceled)

50. (original) Method, according to claim 46, wherein:

the device is modular in construction.

51. (previously presented) Method, according to claim 46, wherein:

the device performs a firewall functionality to protect the Internet-capable appliance.

52. (original) Method, according to claim 46, wherein:

the device incorporates interfaces for ISO contact, contactless, USB and DSL.

53. (new) A compact personal token apparatus, comprising:

a connection module for interfacing the personal token apparatus with an Internet-capable appliance;

a contactless interface;

a translation module for moving signals between the connection module and the contactless interface;

the contactless interface is an RFID interface.

54. (new) The apparatus of claim 53 wherein the connection module is selected from the group consisting of USB, FireWire, IR, Bluetooth, standard serial port, WLAN, and similar interfaces capable of interfacing with the Internet-capable appliance.

55. (new) The apparatus of claim 53 wherein the Internet-capable appliance is selected from the group consisting of personal computer (PC), laptop, PDA, MP3 player, cellphone, and similar Internet-capable devices.

56. (new) The apparatus of claim 53 wherein the contactless interface is selected from the group consisting of ISO 14443, ISO 15693, NFC and similar contactless interfaces.

57. (new) The apparatus of claim 53, further comprising:
a wireless interface.

58. (new) The apparatus of claim 53, further comprising:
an RFID or NFC antenna.

59. (new) Method of linking the virtual world of the Internet with the real world of contactless transactions, comprising:
providing a compact personal token apparatus, comprising:
a connection module for interfacing the personal token apparatus with an Internet-capable appliance;
a contactless RFID interface; and
means for moving signals between the connection module and the contactless interface;
interacting in the virtual world when connected with the Internet-capable appliance; and
interacting in the real world after interacting in the virtual world.

60. (new) The method of claim 59, wherein interacting in the real world comprises an activity selected from the group consisiting of personal identification, secure network logon, access control, e-ticketing, e-payment and similar applications.

Remarks

This is a continuing prosecution (RCE) of 10/990,296 which received a final rejection. An Examiner interview was conducted, by telephone, and it was decided that Applicant would file this RCE, and that an Amendment would be submitted at the same time.

What is sought to be achieved by this Preliminary Amendment is:

1. clarify some of the terminology and concepts used (and discussed, and claimed)
2. present claims that are allowable over the cited references.

References to portions of the specification may be made to page/line of the application and/or to numbered paragraphs [0###] of the published application.

By way of review, the invention is directed to an **apparatus** (former claims 1, 21) and a **method** (former claim 46).

The **apparatus** has
USB interface
wireless interface
contactless interface

USB: is an example of a mechanical (plug) connection with a computer, i.e., a wired connection.

Wireless and **Contactless** are two types of radio frequency (RF) interfaces. In a most general sense, both are "wireless" in that they do not requires wires, and that they use RF. However, in the art to which this invention most nearly pertains, the terms "wireless" and "contactless" have two very different meanings and two very different functionalities. These differences are well pointed out in the specification, as follows.

Regarding **wireless interfaces** ....

As noted in the specification (page __, [0122] glossary),
wireless Technology that allows a user to communicate and/or connect to the Internet or mobile phone networks without physical wires. Wi-Fi, Bluetooth®, CDMA and GSM are all examples of **wireless** technology.

As noted in the specification (page __, [0121] glossary),
Wi-Fi Short for "Wireless Fidelity". **Wireless** technology, also known as 802.11b, that enables you to access the Internet, to send and receive email, and browse the Web anywhere within range of a Wi-Fi access point, or HotSpot.

As noted in the specification (page __, [0045] glossary),
Bluetooth A **wireless** technology developed by Ericsson, Intel, Nokia and Toshiba that specifies how mobile phones, computers and PDAs interconnect with each other, with computers, and with office or home phones. The technology enables data connections between electronic devices in the 2.4 GHz range at 720 Kbps (kilo bits

per second) within a 30-foot range. Bluetooth uses low-power radio frequencies to transfer information wirelessly between similarly equipped devices.

As noted in the specification (page __, [0119] glossary),

UWB UWB is short for "Ultra Wide Band". UWB is a **wireless** communications technology that transmits data in short pulses which are spread out over a wide swath of spectrum. Because the technology does not use a single frequency, UWB enjoys several potential advantages over single-frequency transmissions. For one, it can transmit data in large bursts because data is moving on several channels at once. Another advantage is that it can share frequencies that is used by other applications because it transmits only for extremely short periods, which do not last long enough to cause interference with other signals.

As noted in the specification (page __, [0123] glossary),

WLAN Short for "**wireless** local-area network". Also referred to as LAWN. A WLAN is a type of local-area network that uses high-frequency radio waves rather than wires for communication between nodes (e.g., between PCs).

As noted in the specification (page __, [0072] glossary), ***AMENDED HEREWITH***

IEEE 802.11 The IEEE standard for **wireless** Local Area Networks (LANs). It uses three different physical layers, 802.11a, 802.11b and 802.11g.

The **wireless interfaces** of interest in the present invention are principally WLAN, Bluetooth and UWB. These **wireless** interfaces operate at a distance of several meters, generally for avoiding "cable spaghetti". For example, Bluetooth headsets and other computer peripherals. WLAN is typically used for networking several computers in an office.

Regarding **contactless interfaces** ....

As noted in the specification (page __, [0077] glossary),

ISO 14443 ISO 14443 RFID cards; **contactless** proximity cards operating at 13.56 MHz in up to 5 inches distance. ISO 14443 defines the contactless interface smart card technical specification.

As noted in the specification (page __, [0080] glossary),

ISO 15693 ISO standard for **contactless** integrated circuits, such as used in RF-ID tags. ISO 15693 RFID cards; contactless vicinity cards operating at 13.56 MHz in up to 50 inches distance. (ISO 15693 is typically not used for financial transactions because of its relatively long range as compared with ISO 14443.)

As noted in the specification (page __, [0089] glossary), ***AMENDED HEREWITH***

NFC Short for "Near Field Communication". NFC is a **contactless** connectivity technology that enables short-range communication between electronic devices. If two devices are held close together (for example, a mobile phone and a personal digital assistant), NFC interfaces establish a peer-to-peer protocol, and information such as phone book details can be passed freely between them. NFC devices can be linked to **contactless** smart cards, and can operate like a **contactless** smart card, even when powered down. This means that a mobile phone can operate like a transportation card, and enable fare payment and access to the subway. NFC is an open platform technology standardized in ECMA (European Computer Manufacturers Association) 340 as well as ETSI (European Telecommunications Standards Institute) TS 102 190 V1.1.1 and ISO/IEC 18092. These standards specify the modulation schemes, coding, transfer speeds, and frame format of the RF interface of NFC devices, as well as initialisation schemes and conditions required for data collision-control during initialisation – for both passive and active modes.

As noted in the specification (page __, [0101] glossary),

RFID Short for "Radio Frequency Identification". An RFID device interacts, typically at a limited distance, with a "reader", and may be either "passive" (powered by the reader) or "active" (having its own power source, such as a battery).

The **contactless interfaces** of interest in the present invention are principally **RFID** contactless interfaces such as **ISO 14443, 15693 and NFC**. **RFID** operates at a maximum distance of 1 meter for purposes of identification. In a payment (financial transaction) application, the distance is restricted to 10 cm.

There are clear distinctions between **wireless** and **contactless**, for example (Specification, [0134]):

> The apparatus may further comprise a standard-compliant contactless/wireless interface; the contactless/wireless interface complying to one or more of the following standard interfaces: RFID-contactless interface according to ISO 14443 and ISO 15693 as well as similar interfaces, Bluetooth compatible interface, WLAN 802.11, UWB, and any similar interface.

Parsing the paragraph [0134], please note: **contactless** / wireless .....
.... (re contactless) " **RFID-contactless interface according to ISO 14443 and ISO 15693 as well as similar interfaces**"
.... (re wireless) "**Bluetooth compatible interface, WLAN 802.11, UWB, and any similar interface**."

This paragraph [0134] is re-written herewith, as follows ...
The apparatus may further comprise a standard–compliant contactless ~~/wireless interface; the contactless/wireless~~ interface complying to one or more of the following standard interfaces: RFID-contactless interface according to ISO 14443 and ISO 15693 as well as similar interfaces, and a wireless interface complying to one or more of the following standard interfaces: Bluetooth compatible interface, WLAN ~~812.11~~ 802.11, UWB, and any similar interface.

A **wireless** connection (e.g., WLAN) is generally simply a substitute for a physical (e.g., USB) connection between the apparatus and an Internet-capable appliance, allowing the user some flexibility of movement. For example, see the specification, [0131]:

> According to the invention, a compact personal token apparatus comprises a connection module; a translation module; a processor module; and an input/output module. The connection module is for interfacing the personal token apparatus with a an Internet-capable

appliance; and the interface is selected from the group consisting of **USB, FireWire, IR, Bluetooth, standard serial port, WLAN.**

Wireless and **contactless** are different than one another, although both use radio frequency. They are different communications protocols with different capablities and are used for different purposes. For example, a contactless RFID smart card protocol according to ISO 14443 and ISO 15693, can be used for private, secure financial transactions in "real world" applications such as payment at a retailer.

Note, for example, that 50 inches (ISO 15693, an RFID contactless protocol) is considered to be too great a distance to provide appropriate security for (**contactless**) financial transactions.

But 50 inches would not be enough to provide a (**wireless**) network betwen office computers!

Additionally, generally, **contactless** technology is primarily passive (having no power source of its own), deriving power to operate from the electromagnetic field generated by a nearby reader.

Wireless technologies, on the other hand, generally require a their own power source (either batteries, or plugged in) to operate.

Contactless is different than **wireless**. different protocol, different signal characteristics, different utility, different energy requirments, different capabilities, different purposes, different advantages, different limitations. They are different.

Amendments to the Specification

In a few places, "802.11" had a ***typo*** and was "812.11". (It was correctly stated as "802.11" in other places in the specification, and is generally widely known to be "802.11")

Certainly, in a broad historical sense the term "wireless" has been used by many to indicate any interface (typically electromagnetic) that does not involve wired connections. However, the glossary is replete with industry-standard definitions which clarify the distinction between "wireless" (such as 802.11) and "contactless" (such as ISO 14443, 15693 and NFC).

The distinction between "wireless" and "contactless" may have been a little indistinct in places, and various amendments are made to the specification herewith to avoid possible confusion.

There is ample support throughout the specification for the changes made herein. For example, in the several glossary entries noted above, as well as in the text, for example at [0264] "When a user enters a hot zone area equipped with a Wi-Fi / 802.11 **wireless** local area network ..."

No new matter is entered by these amendments.

Distinguishing the Invention from the Cited Art

As noted above, the apparatus (in its broadest sense) generally comprises:
a USB interface
a wireless interface

a contactless interface

The Cited References

The cited references are Margalit (6,748,541) and Jiau (2003/026821)

Margalit has
USB interface
contains a 7816 smart card chip (Fig. 2, 170)
no wireless
no contactless

As noted in the specification of the present invention, (page __, line __ [0079]),
ISO 7816 Regarding smart card, ISO7816 defines specification of **contact** interface IC chip and IC card.

Margalit's smart card chip is an "ISO7816 memory" (Margalit column 3, line 63)

Margalit is a **contact** device. It is neither **contactless**, nor **wireless**.

Margalit's USB plug device of FIG. 2 includes both a CPU and a smart card chip (ICC) memory 170, typically a ISO7816 (T=0/1) protocol-based chip communicating with the CPU 130 using an ISO7816-3 protocol. The apparatus of FIG. 2 is similar to the apparatus of FIG. 1 except that no separate user's data memory 70 is provided. (Margalit column 5, lines 6-11)

Margalit's flow of data in the apparatus of FIG. 2 typically comprises the following flow:

> The USB interface chip 140 gets USB packets from the USB host 120. The USB interface chip 140 parses the data and passes it to the microprocessor 130. The data, which typically comprises a ISO7816-3 T=0/1 formatted packet, is passed by the microprocessor to the smart-card 170 in a ISO7816-3 protocol. The microprocessor 130 gets the response from the smart card 160 and passes the data to the USB interface chip 140. The USB interface chip 140 wraps the data in USB packet format and passes it to the host 120. (Margalit column 6, lines 17-27)

Margalit has:
a USB interface
a CPU
memory (which may reside in the 7816 memory)
some 7816 smart card type functionality

Margalit does not have:
wireless interface
contactless interface:

Funtionally, the present invention provides ...
interacting with the "virtual world", over the internet, with a computer, either by
USB or wireless (see, e.g., claim 47) and
interacting in the "real world" using contactless RFID interface (see, e.g., claim 33)

Margalit cannot interact in both the "virtual" world (Internet), via plug in (USB) or wireless connection, which it has - combined with - performing in the "real" world of RFID contactless applications, which Margalit does not have. And, there is no "suggestion to try" (such as combine with an RFID reference), or to go in that direction.

Jiau discloses a body wearable personal network server (BWPNS) device which can communicate via **wireless** in the form of personal area network (Bluetooth) and **wireless** LAN (IEEE 802.11), and has a USB plug

Jiau does not have, nor does Jiau suggest combining a "RFID-contactless interface according to ISO 14443 and ISO 15693 as well as similar interfaces". The invention does.

Since Jiau is lacking in a key element of the present invention - namely, contactless RFID interface, it does not suggest the present invention, either alone or in combination with Margalit which also does not have any contactless or even a wireless interface. And, Jiau does not suggest combining any 7816 smart card type functionality. Even if there were a suggestion to combine these two references, the invention would not be rendered obvious by the combination.

It thus appears that the following claims are patentable in light of the references cited.

Proposed "claims"

It would appear that claims along the following lines should be allowed.
An amendment to the claims is included herewith.

X. A compact personal token apparatus, comprising:

a connection module (for example, USB) for interfacing the personal token apparatus with an Internet-capable appliance; (see original claims 1, 3)

a contactless interface;

a translation module for moving signals between the connection module (USB interface) and the contactless interface; (see original claims 1, 4)

the contactless interface is an RFID interface selected from the group consisting of ISO 14443 (RFID-contactless interface), ISO 15693 (RFID-contactless interface), NFC and similar contactless interfaces. (see original claim 5)

Y. The apparatus of claim X, further comprising:

a wireless interface; and

the wireless interface is selected from the group consisting of WLAN, Bluetooth, UWB, and similar wireless interfaces. (see original claim 23)

support may be found in the specification at paragraph [0134]

> The apparatus may further comprise a standard–compliant contactless/wireless interface; the contactless/wireless interface complying to one or more of the following standard interfaces: RFID-contactless interface according to ISO 14443 and ISO 15693 as well as similar interfaces, Bluetooth compatible interface, WLAN 812.11, UWB, and any similar interface.

The device (smart fob, USB key fob) can function as a Multi-Interface Reader-less Device to provide for physical and logical access control. This embodiment would include an RFID or NFC (Near Field Communication) antenna.

Thus, claim **X** is directed to **the contactless interface** which permits the user to wander around in the "real" world (at retailers, for example) to conduct secure (such as financial) transactions. None of the cited references disclose this.

The connection module (such as USB), alternatively the wireless interface (see next claim **Y**) allows the user to update the fob when plugged into a computer, such as for downloading value from the Internet ("virtual" world).

Dependent Claim **Y** is directed to **wireless** communication over long distances, without plugging into the computer. Using, for example, the Bluetooth interface of claim Y, the RFID feature of claim **X** can communicate via a PC over the Internet.

The claims are amended herewith, along the lines discussed hereinabove. It is believed that they now distinguish over the cited references (Margalit, Jiau).

Claim 1 is amended to include interfacing to the Internet (former claim 2) and moving signals to the contactless interface.

Claim 2 is amended to recite Internet-capable appliances (former claim 3) and recites possible interfaces used by the connection module.

Claim 3 is limited to a USB connection with the Internet-capable appliance.

Regarding clain 13, see paragraph [023], page 34.

Regarding claim 46, see claim 49.

Regarding claim 59, see for example, paragraph [0137] page 25
The apparatus may further comprise a dual interface chip (processor) inside the personal token which can be directly programmed by a software running on the host system using the interface processor without the need for an external contact based dual interface read/write device. The software may be web based, allowing for downloading information from the web directly into the dual interface processor memory (for example, event tickets) thus linking the virtual world to the real world. The downloaded information may be used in the real world by using the contactless RFID interface.
See also claim 36, as filed.

Regarding claim 60, see claim 35 (as filed).

Newly-Presented Claims, and Claim Count

The highest number of claims previously paid for is:
52 total claims

3 independent claims (1,21,46)

Dependent claims 34 and 49 are canceled.
Claim 21 (formerly independent) is amended to be in dependent form.
Claims 53-60 are presented herewith, including two independent claims (53, 59).

After entering this amendment, there will be:
58 total claims
4 independent claims

Thus, necessitating excess claim(s) fee(s) for:
6 total claims @$25 = **$150** (small entity)
1 independent claim = **$100** (small entity)

The fee for entering an RCE is **$395** (small entity)

Conclusion

The claims should be allowed.
The amendments to the specification should be entered.
No new matter is entered by this amendment.

For the Applicant,

DAStauffer

Dwight A. Stauffer
Registered Patent Agent # 47,963

Customer 37053
D.A. Stauffer Patent Services LLC
1006 Montford Rd.
Cleveland Hts. OH 44121
(216) 381-6599

Electronic Patent Application Fee Transmittal

Application Number:	10990296
Filing Date:	16-Nov-2004
Title of Invention:	Multi-interface compact personal token apparatus and methods of use
First Named Inventor:	Dennis J. Ryan
Filer:	Dwight A. Stauffer
Attorney Docket Number:	Ryan C-4

Filed as Small Entity

Utility Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Claims in excess of 20	2202	6	25	150
Independent claims in excess of 3	2201	1	100	100
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Extension-of-Time:				
Miscellaneous:				
Request for continued examination	2801	1	395	395
	Total in USD ($)			**645**

Electronic Acknowledgement Receipt

EFS ID:	1031229
Application Number:	10990296
Confirmation Number:	2050
Title of Invention:	Multi-interface compact personal token apparatus and methods of use
First Named Inventor:	Dennis J. Ryan
Customer Number:	37053
Filer:	Dwight A. Stauffer
Filer Authorized By:	
Attorney Docket Number:	Ryan C-4
Receipt Date:	25-APR-2006
Filing Date:	16-NOV-2004
Time Stamp:	23:39:14
Application Type:	Utility
International Application Number:	

Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	$ 645.0
RAM confirmation Number	320
Deposit Account	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part	Pages

1		Ryan_C-4_rce_and_Amendment_as_filed_4-25-06.pdf	357802	yes	26
	Multipart Description				
	Doc Desc		**Start**	**End**	
	Request for Continued Examination (RCE)		1	1	
	Specification		2	8	
	Claims		9	18	
	Applicant Arguments/Remarks Made in an Amendment		19	26	
Warnings:					
Information:					
2	Fee Worksheet (PTO-875)	fee-info.pdf	8432	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	366234		

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

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

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

substitute forms PTO/SB/08a & PTO/SB/08b

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Sheet 1 OF 3

Application Number	**10/990,296**
Filing Date	**November 16, 2004**
First Named Inventor	Dennis J. Ryan
Art Unit	2876
Examiner Name	Uyen Chau N. Lee
Practitioner Docket No.	Ryan C-4

U.S. PATENT DOCUMENTS

Exam. Initials	Cite No.	Document Number No. -Kind Code (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Relevant Pages, Columns, Lines
	A	US-3,941,489	03-22-1974	Bryan	
	B	US-4,367,965	01-11-1983	Speitel et al.	
	C	US-5,761,648	06-02-1998	Golden et al.	
	D	US-6,067,235	05-23-2000	Finn et al.	
	E	US 6,085,320	07-04-2000	Kaliski, Jr.	
	F	US 6,148,354	11-14-2000	Ban et al.	
	G	US 6,168,077	01-02-2001	Gray et al.	
	H	US 6,189,098	02-13-2001	Kaliski, Jr.	
	I	US 6,240,184	05-29-2001	Huynh et al.	
	J	US 6,283,658	09-04-2001	Estevez et al.	
	K	US 6,370,603	04-09-2002	Silverman et al.	
	L	US 6,385,677	05-07-2002	Yao	
	M	US 6,505,773	01-14-2003	Palmer et al.	
	N	US 6,543,690	04-08-2003	Leydier et al.	
	O	US 6,567,273	05-20-2003	Liu et al.	
	P	US 6,658,516	12-02-2003	Yao	
	Q	US 6,694,399	02-17-2004	Leydier et al.	
	R	US 6,724,680	04-20-2004	Ng et al.	
	S	US 6,748,541	06-08-2004	Margalit et al.	
	T	US 6,752,321	06-22-2004	Leaming	
	U	US 6,763,399	07-13-2004	Margalit et al.	
	V	US 6,772,956	08-10-2004	Leaming	
	W	US 6,798,169	09-28-2004	Stratmann et al.	
	X	US 6,801,956	10-05-2004	Feuser et al.	
	Y	US 6,848,045	01-25-2005	Long et al.	
	Z	US 6,876,420	04-05-2005	Hong et al.	
	AA	US 6,879,597	04-12-2005	Tordera et al.	
	BB	US 2001 0043702	11-22-2001	Elteto et al.	
	CC	US 2001 0054148	12-20-2001	Hoornaert	
	DD	US 2002 0011516	01-31-2002	Lee	
	EE	US 2003 0000267	01-02-2003	Jacob et al.	
	FF	US 2003 0028797	02-06-2003	Long et al.	
	GG	US 2003 0087601	05-08-2003	Agam et al.	
	HH	US 2003 0102380	06-05-2003	Spencer	
	II	US 2003 0236821	12-25-2003	Jiau	
	JJ	US 6,342,839	01-29-2002	Curkendall et al.	

Examiner Signature

Date Considered

substitute forms PTO/SB/08a & PTO/SB/08b

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

Sheet 2 OF 3

Application Number	**10/990,296**
Filing Date	**November 16, 2004**
First Named Inventor	Dennis J. Ryan
Art Unit	2876
Examiner Name	Uyen Chau N. Lee
Practitioner Docket No.	Ryan C-4

FOREIGN PATENT DOCUMENTS

Exam. Initials	Cite No.	Foreign Patent Document Country Code-Number-Kind Code	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Doc.	Relevant Pages, Columns, Lines	T
	f1	DE19631050	02-05-1998	Bergler et al.	Drawings	
	f2	HK 1063994				T
	f3	HK 1063995				T
	f4	JP2004246720	09-02-2004		Drawings	
	f5	WO99 052051	10-14-1999	International Business Machines		T
	f6	WO99 038062	07-29-1999	Kobil Computer GMBH	Abs.(Engl), Dwg.	
	f7	WO00 036252	06-22-2000	Jacob	Abs.(Engl), Dwg.	
	f8	WO00 042491	07-20-2000	Rainbow Technologies, Inc.		T
	f9	WO00 065180	11-02-2000	Muller et al.	Abs.(Engl), Dwg.	
	f10	WO00 075755	12-14-2000	Eutron Infosecurities		T
	f11	WO01 014179	03-01-2001	Wittwer et al.	Abs.(Engl), Dwg.	
	f12	WO01 038673	03-31-2001	Wittwer et al.	Abs.(Engl), Dwg.	
	f13	WO01 039102	11-02-2001	Muller et al.		T
	f14	WO01 048339	07-05-2001	Jacob et al.	Abs.(Engl), Dwg.	
	f15	WO01 048342	07-05-2001	Jacob et al.	Abs.(Engl), Dwg.	
	f16	WO01 061692	08-23-2001	Trek Technology		T
	f17	WO01 088693	11-22-2001	Seysen	Abs.(Engl), Dwg.	
	f18	WO01 096990	12-20-2001	Rainbow Technologies, Inc.		T
	f19	WO03 014887	02-20-2003	Activcard Ireland		T
	f20	WO03 034189	04-23-2003	Activcard Ireland		T
	f21	WO04 002058	12-31-2003	Gemplus	Abs.(Engl), Dwg.	
	f22	WO04 081706	09-23-2004	Digisafe Ltd.		T
	f23	WO04 081769	09-24-2004	Axalto SA		T

NON PATENT LITERATURE DOCUMENTS

Exam. Initials	Cite No.	Name of author (ALL-CAPS), title of article, title of item, date, pages, vol-issue #, publisher, city and/or country where published.	T
	1	*ACR38CT Contactless SIM Tracker Technical Specification*, Advanced Card Systems Ltd., Hong Kong.	T
	2	*ACR38DT Dual Key Technical Specifications, Version 1.3*, September 2004, Advanced Card Systems Ltd., Hong Kong.	T

Examiner Signature

Date Considered

substitute forms PTO/SB/08a & PTO/SB/08b **INFORMATION DISCLOSURE STATEMENT BY APPLICANT**		Application Number	**10/990,296**
		Filing Date	**November 16, 2004**
		First Named Inventor	Dennis J. Ryan
		Art Unit	2876
		Examiner Name	Uyen Chau N. Lee
Sheet 3 OF 3		Practitioner Docket No.	Ryan C-4

NON PATENT LITERATURE DOCUMENTS

Exam. Initials	Cite No.	Name of author (ALL-CAPS), title of article, title of item, date, pages, vol-issue #, publisher, city and/or country where published.	T
	3	*Dallas Semiconductor DS1490F 2-in-1 Fob*, Dallas Semiconductor, Dallas TX.	T
	4	*Dallas Semiconductor DS9490R-DS9490B USB to 1-Wire/iButton Adaptor*, Maxim I-C, Sunnyvale CA.	T
	5	HARA, YOSHIKO, *Matsushita blends FERAM technology with smart cards*, EE Times, October 1, 2004, CMP Media, Manhasset NY.	T
	6	*Japan's Matsushita developing memory cards with smart chip function*, October 1, 2004, Mercury News, San Jose CA.	T
	7	*OTi-6828 Flash Disk Controller*, Ours Technology Inc., Taiwan.	T
	8	*Panasonic Develops RFID smartSD Card*, October 4, 2004, Palminfocenter.com, Sunnyvale CA.	T
	9	*Panasonic Develops Industry's First SD Memory Card with Contacless Smart Card Capabilities*, October 1, 2004, The Japan Corporate News Network, Tokyo.	T
	10	ROJAS, PETER, *Panasonic's Smart SD adds RFID to the mix*, October 4, 2004, Engadget LLC, New York NY.	T
	11	*Delivering ultimate security, high performance and ultra low power consumption, SmartMX is now in volume supply*, November 18-20, 2003, Cartes 2003, aris Nort Villepinte, France	T
	12	BALABAN, DAN, *Digital Rights pits SIMS against Flash Cards, Card Technology*, November 2004, pp 24, 25, 26, 28, 30, Card Technology, Chicago IL.	T
	13	*Smart MX P5CT072 Secure Dual Interface PKI Smart Card Controller, Rev. 1.3*, October 2004, Koninklijke Philips Electronics NV, The Netherlands	T
	14	*Vodafone KK Develops Contactless Smart Card Mobile Handset*, May 6, 2004, HiTEK Magazine, Dubai	T
	15	*SmartSD Card Structure,* Panasonic	T

Examiner Signature

Date Considered

(19) BUNDESREPUBLIK DEUTSCHLAND

DEUTSCHES PATENTAMT

(12) Offenlegungsschrift

(10) DE 196 31 050 A1

(51) Int. Cl.⁶:
H 04 L 25/20
H 04 L 12/40
H 04 L 29/10
G 08 C 15/00
G 08 C 19/16
G 06 F 13/00

(21) Aktenzeichen: 196 31 050.4
(22) Anmeldetag: 1. 8. 96
(43) Offenlegungstag: 5. 2. 98

(71) Anmelder:
Bergler, Frank, 75223 Niefern-Öschelbronn, DE;
Käuffert, Uwe, 75180 Pforzheim, DE

(72) Erfinder:
gleich Anmelder

(56) Entgegenhaltungen:

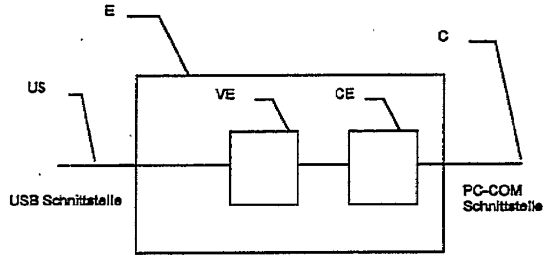
DE	39 31 511 C2
DE	41 15 242 A1
DE	33 22 690 A1
US	50 86 385 A
EP	0 17 035 A1

STRASS,Hermann: Universell, seriell, aber kein Bus. In: Elektronik 20, 1995, S.32-34,38-42;
LANGER,Klaus,D.: Softwareverareitung der HDLC-Ebene bitorientierter Protokolle. In: ntz, Bd. 39, 1986, H. 11, S.760,762-764,766,767;
STRASS,Hermann: Neue Stecker braucht das Land. in: DOS, Juli 1996, S.16,18;

Prüfungsantrag gem. § 44 PatG ist gestellt

(54) Schnittstellenkonverter für USB

(57) Die Universal Serial Bus Schnittstelle soll auf eine andere Schnittstelle umgesetzt werden.
Die Daten von und zur USB Schnittstelle werden in einer erfindungsgemäß realisierten Einrichtung einer Verarbeitungseinheit zugeführt, entsprechend dem USB Protokoll behandelt, in ein anderes geeignetes Übertragungsprotokoll umgesetzt und dann einer anderen nicht nach USB Standard ausgelegten Schnittstelle zugeführt. Diese Schnittstelle kann zum Beispiel eine PC-COM Schnittstelle sein.



Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

BUNDESDRUCKEREI 12.97 702 066/284 3/27

Beschreibung

Die vorliegende Erfindung betrifft eine Einrichtung zur bidirektionalen Umsetzung von Signalen zwischen einer USB Schnittstelle und einer anderen Schnittstelle.

Die Universal Serial BUS, USB, ist in der Spezifikation, Revision 1.0 vom 1 Januar 1996 beschrieben; und ist in der vorliegenden Ausgabe der Revision 1.0 öffentlich und für jedermann zugänglich.

Diese Spezifikation beschreibt sowohl die logische Struktur der USB Schnittstelle inklusive der notwendigen Protokolle, Signalisierung und Timinganforderungen als auch die physikalische Struktur. Als physikalisches Übertragungsmedium wird ausschließlich die elektrische Übertragung über ein elektrisch leitendes Kabel definiert.

Der USB Schnittstellenstandard ist ein kabelgebundener Übertragungsstandard, der insbesondere die verschiedenen Anschlußeinheiten wie Tastatur, Maus, Drucker, Video, Audio und sonstige Zusatzeinrichtungen für Workstations und PCs einheitlich mit der Zentraleinheit verbinden soll.

Bekannt sind Protokollumsetzer zwischen unterschiedlichen logischen und physikalischen Schnittstellen. Ein aus dem Stand der Technik bekannter Protokollumsetzer für ISDN konvertiert das nationale 1TR6 Protokoll auf der Benutzerseite in das europäische DSS1 auf der Netzseite.

Stand der Technik ist, daß für diese Anbindung jeweils auf die Aufgabenstellung zugeschnittene Standards verwendet werden, z. B. LPT zur Verbindung von Druckern mit PCs.

Der Erfindung liegt die Aufgabe zugrunde existierende Ein-/Ausgabeeinrichtungen, die nach einem anderen Standard als dem USB Standard arbeiten an den USB Standard anzupassen.

Diese Aufgabe wird erfindungsgemäß dadurch gelöst, daß die auf der USB Schnittstelle kommenden Daten empfangen und auf die andere Schnittstelle umgesetzt werden. Die Signale auf der anderen Schnittstelle werden ebenfalls empfangen und auf die USB Schnittstelle umgesetzt. Alle Anforderungen der USB Spezifikation werden dabei erfüllt.

Im Folgenden wird die Erfindung anhand eines Ausführungsbeispiels für eine Umsetzung auf die PC-COM Schnittstelle und anhand von einer Figur näher erläutert.

Fig. 1 Blockschaltbild.

Die erfindungsgemäß realisierte Einrichtung (E) weist gemäß **Fig.** 1 eine USB Schnittstelle auf und eine PC-COM Schnittstelle. Die Daten der PC-COM Schnittstelle (C) werden an die COM Einheit (CE) weitergeleitet. In der nachgeschalteten Verarbeitungseinheit (VE) werden die Daten auf das USB Protokoll umgesetzt und über die USB Schnittstelle (US) ausgegeben.

Die an der USB Schnittstelle ankommenden Daten werden gemäß der USB Spezifikation und dem vorgeschriebenen Protokoll empfangen, einer Verarbeitungseinheit (VE), welche ein Mikroprozessor oder ein Digitaler Signalprozessor DSP sein kann zugeführt. In dieser Verarbeitungseinheit (VE) werden die Daten ggf. in das für die Übertragung erforderliche Format und Protokoll umgesetzt und anschließend der COM Einheit (CE) zugeführt, um von dort über die COM Schnittstelle (C) übertragen zu werden.

Patentansprüche

1. Einrichtung zur bidirektionalen Umsetzung einer oder mehrerer Schnittstellen nach der Spezifikation Universal Serial BUS, USB, Revision 1.0 vom 15. Januar 1996 und zukünftiger Ausgaben dieser Spezifikation und anderer Spezifikationen welche die Universal Serial Bus Schnittstelle beschreiben auf eine oder mehrere PC-COM Schnittstellen nach V24 und RS232 Standard, **dadurch gekennzeichnet,** daß sowohl das standardisierte Übertragungsprotokoll als auch die elektrischen Parameter für die jeweilige Schnittstelle eingehalten werden.
2. Einrichtung zur bidirektionalen Umsetzung einer oder mehrerer Schnittstellen nach der Spezifikation Universal Serial BUS, USB, Revision 1.0 vom 15. Januar 1996 und zukünftiger Ausgaben dieser Spezifikation und anderer Spezifikationen welche die Universal Serial Bus Schnittstelle beschreiben auf eine oder mehrere PC-LPT Drucker Schnittstellen nach Centronics Standard, dadurch gekennzeichnet, daß sowohl das standardisierte Übertragungsprotokoll als auch die elektrischen Parameter für die jeweilige Schnittstelle eingehalten werden.
3. Einrichtung zur bidirektionalen Umsetzung einer oder mehrerer Schnittstellen nach der Spezifikation Universal Serial BUS, USB, Revision 1.0 vom 15. Januar 1996 und zukünftiger Ausgaben dieser Spezifikation und anderer Spezifikationen welche die Universal Serial Bus Schnittstelle beschreiben auf eine oder mehrere CAN Bus Schnittstellen, dadurch gekennzeichnet, daß sowohl das standardisierte Übertragungsprotokoll als auch die elektrischen Parameter für die jeweilige Schnittstelle eingehalten werden.
4. Einrichtung zur bidirektionalen Umsetzung einer oder mehrerer Schnittstellen nach der Spezifikation Universal Serial BUS, USB, Revision 1.0 vom 15. Januar 1996 und zukünftiger Ausgaben dieser Spezifikation und anderer Spezifikationen welche die Universal Serial Bus Schnittstelle beschreiben auf eine oder mehrere LAN Schnittstellen nach Ethernet oder Token Ring Standard, dadurch gekennzeichnet, daß sowohl das standardisierte Übertragungsprotokoll als auch die elektrischen Parameter für die jeweilige Schnittstelle eingehalten werden.
5. Einrichtung zur bidirektionalen Umsetzung einer oder mehrerer Schnittstellen nach der Spezifikation Universal Serial BUS, USB, Revision 1.0 vom 15. Januar 1996 und zukünftiger Ausgaben dieser Spezifikation und anderer Spezifikationen welche die Universal Serial Bus Schnittstelle beschreiben auf eine oder mehrere GGI oder CHI Schnittstellen, dadurch gekennzeichnet, daß sowohl das standardisierte Übertragungsprotokoll als auch die elektrischen Parameter für die jeweilige Schnittstelle eingehalten werden.
6. Einrichtung zur bidirektionalen Umsetzung einer oder mehrerer Schnittstellen nach der Spezifikation Universal Serial BUS, USB„ Revision 1.0 vom 15. Januar 1996 und zukünftiger Ausgaben dieser Spezifikation und anderer Spezifikationen welche die Universal Serial Bus Schnittstelle beschreiben auf eine oder mehrere PCMCIA Schnittstellen, dadurch gekennzeichnet, daß sowohl das standardisierte Übertragungsprotokoll als auch die elektrischen Parameter für die jeweilige Schnittstelle eingehalten werden.

7. Einrichtung nach mindestens einem der Ansprüche 1—6, dadurch gekennzeichnet, daß eine der USB Schnittstellen auf mindestens 2 unterschiedliche der in den Ansprüchen 1—6 aufgeführten anderen Schnittstellen in der Einrichtung umgesetzt wird.

Hierzu 1 Seite(n) Zeichnungen

Nummer: DE 196 31 050 A1
Int. Cl.^{6}: H 04 L 25/20
Offenlegungstag: 5. Februar 1998

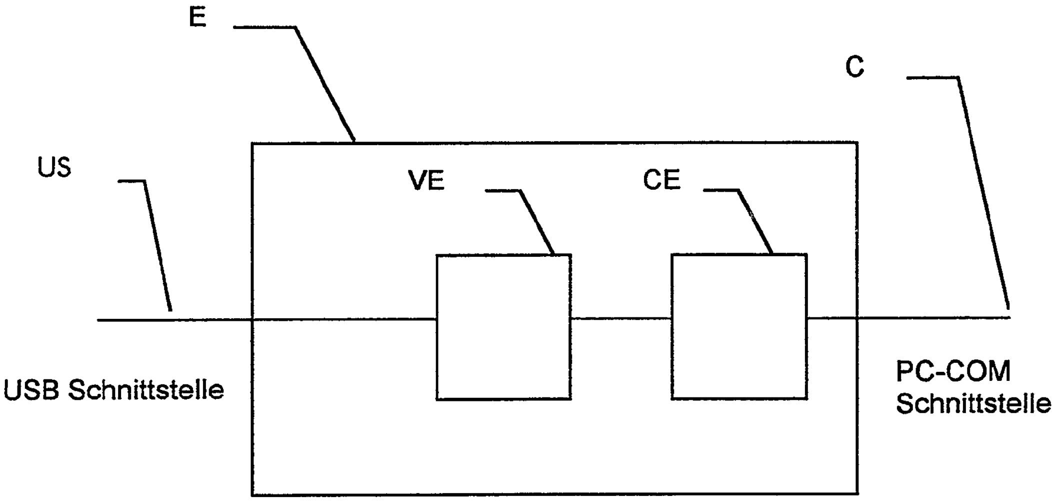


Fig. 1

TITLE

SMART CARD READER WITH CONTACTLESS ACCESS CAPABILITY

FIELD OF INVENTION

This invention relates to an electronic apparatus, and in particular smart-card readers for the dual-mode contact/contactless smart cards.

BACKGROUND OF INVENTION

A smart card consists of an IC chip typically embedded in a flat enclosure. It comes with two popular form factors. One of them is the size of a credit card which is widely used in banking and national ID card projects. The other form factor is the smaller subscriber identification module (SIM card) used in mobile phone. The IC chip itself can simply be a memory chip or a microprocessor chip. Typically, a smart card has eight electric pins which are generally referred to as C1 to C8 to communicate to the external world. Their roles and functions are defined in ISO7816 international standard. A smart card reader is a device that will make electrical contact with each of these pins, so that an external host device can communicate with the smart card through the reader. Out of these 8 pins, ISO7816 standard defines 6 of them for the use of carrying electric power, the clock and reset signals as well as data input and data output signals between the reader and the card. Pins C4 and C8 are not defined and some manufacturers are using these 2 pins to carry out special functions, which will be described later. This type of smart card is said to operate in a contact mode, as it needs to make physical contact with the card reader in order for it to get the electrical power and to communicate with the external world.

There is another kind of smart card that can operate in a contactless mode. It is based on the Radio Frequency Identification (RFID) technology. In this case, the contactless smart card reader, also known as the interrogator, sends out the Radio Frequency (RF) signal. The contactless smart card has an antenna and RF circuitry which is tuned to receive the RF signal at this frequency. When the contactless card is in the vicinity of the interrogator, it picks up the RF signal, and uses it to power the analogue and digital circuitry within the smart card IC. The interrogator and the contactless smart card also communicate with each other through the same RF channel. The International Standardization Organization (ISO) has published a few standards that stipulate the specifications of contactless smart card operations in detail. They are the ISO14443-type A and type B standards, where the reading distance can be up to 10 cm, as well as the ISO15693 standard where the reading distance is extended to 15 cm or longer. Other vendors adopt the same operating principle but employ their own proprietary standards.

The contactless smart card operates according to the near-field wave propagation principle of the electromagnetic wave theory. Typically, inductive coupling is adopted in this case whereby the RF magnetic field generated by the interrogator induces electric current at the contactless smart card when it moves in the vicinity of the interrogator. To maximize magnetic field coupling, both the antennas of the interrogator and the contactless smart card are arranged in the form of cylindrical loop that consists of multiple turns of electrical wires. At the 13.56MHz frequency specified by the ISO standards, the antenna of the contactless smart card comprises just a few turns. These few turns can be placed along the perimeter of the rectangular shape of a normal size smart card.

Smart cards operating in contact mode have been widely used in many applications where security and privacy are the prime concerns. These include banking transaction, credit card processing, on-line electronic commerce, logical access to computer systems, as well as national identification card projects, health care and social security card projects. Another mass adoption of smart card technology is the subscriber identification card (SIM card) used in the GSM mobile phone handsets. On the other hands, contactless smart card technology is more convenient to use, as users do not need to physically insert the smart card into the card reader. Hence, it is widely used in physical access control, micro-payment of mass transit systems among many other applications. However, the latter technology may not offer the same level of security protection as the contact mode of operation, because the wireless data transmission could be eavesdropped by a rogue contactless reader located in close proximity of the genuine one.

As a result, vendors have developed a dual-mode smart card that can operate in either contact mode or contactless mode. This card, also known as combi-card, normally has a form factor that is the same size as a normal credit card. It has 8 pin connections as per normal contact smart card which can connect to a smart card reader in contact mode of operation. It also has an embedded antenna inside the card so that it can function as a contactless card by itself.

Such a dual-mode smart card would require a smart card reader for it to perform the contact-mode operation. Unfortunately, not many computer systems carry a smart card reader as their standard peripheral device. However, most computer systems support serial and USB (Universal Serial Bus) ports. Hence, it is desirable to have a device that has a built-in smart card reader to interface with the dual-mode smart card on the one hand, and a USB or serial port to connect to a computer system on the other. If such a device needs to accommodate a credit-card size combi-card, it will be cumbersome for users to carry. Therefore, a dual-mode smart card having the SIM form factor is much preferred. This will enable many new applications. For example, users can store secret keys and password information inside the dual-mode SIM sized smart card. When the user wants to log on to a computer system, he can connect the device to a USB port. A software program can be automatically initiated to authenticate the user and allow him access to the computer. When the user wants to access certain restricted premises, it can function in contactless mode as a physical access device for the user. In another application scenario, the dual-mode smart card can be configured as a store-value card. The user can use the contact-mode of operation to top up the stored value, and use the contactless-mode of operation to pay service fee. The contact-mode ensures high security while the contactless-mode offers user convenience. In fact, the device can be made small enough as a personal electronic key that is always carried by the user in his key-chain.

However, for a dual mode smart card that has a form factor of a SIM card, the loop antenna has to be placed outside the SIM card, as the area encompassing the SIM card is too small to capture sufficient magnetic flux from the interrogator to power the smart card IC. Some manufacturers makes use of pins C4 and C8, the two pins that are not defined in the ISO7816 standard, to connect the SIM card to the external antenna. Hence it is necessary to design and develop an antenna and its associated circuitry, and incorporate such antenna assembly to the device in the most cost-effective manner without compromising its RF reception quality.

SUMMARY OF INVENTION

In view of the foregoing background, it is therefore an object of the present invention to provide an improved apparatus that provides access to a dual-mode smart card either through a smart card reader electronic module to an external host in contact mode of operation, or through an antenna assembly to a contactless card reader in contactless mode of operation. Accordingly, the present invention provides an apparatus comprising the electronic circuitry of a smart-card reader that is adapted to connect to a dual-mode smart card in a contact mode via a smart card connector, and an antenna assembly adapted to connect to the smart card connector for contactless mode operation.

In the preferred embodiment, the entire circuitry of the smart-card reader and the antenna assembly is fabricated in a single printed circuit board so that it can reduce the production cost and improve the reliability. The antenna circuitry may comprise a loop antenna, or it may include other electronic components such as a tuning capacitor. The antenna may be fabricated as thin electrical lines running in loops around the perimeter of the printed circuit board. The circuitry of the smart card reader may be placed at the inner portion of the printed circuit board.

Another aspect of the present invention is to fabricate the antenna in the inner layers of a multi-layer printed circuit board. The loop antenna assembly may occupy more than one layer, with the antenna wire in one layer electrically connected to another layer via electrically conducting through-holes in the printed circuit board so that the multi-layer wiring loops constitutes a single loop antenna.

In a second preferred embodiment, the loop antenna may be embedded in the casing that houses the apparatus. The antenna wiring may be embedded in the casing, and its leads make electrical connection to the rest of the antenna assembly in the printed circuit board. This may minimize the number of layers of printed circuit board.

A method aspect of the present invention is for forming the antenna assembly. The method preferably comprises the steps of: constructing metal connectors in a printed circuit board to realize the circuit diagram of the smart card reader electronic module, embedding at least one metal wire around the perimeter of the printed circuit board, and electrically connecting the metal wire to the smart card connector so that the metal wire functions as an antenna for the antenna assembly for contactless mode operation.

It should be noted that the metal conductors that realize the circuit diagram of the smart card reader electronic module should not form closed loops. Moreover, for a multi-layer printed circuit board, the metal wire for the antenna may occupy more than one layers. In such case, electrically conducting pin-holes will be used to connect wires from multiple layers together so that it constitutes a single antenna.

Another prefer method embodiment comprises the steps of: embedding the smart card reader module on the printed circuit board and embedding the loop antenna on the casing of the apparatus, and electrically connecting the loop antenna to the rest of the antenna assembly.

Another method aspect of the present invention is for accessing the content of the dual-mode smart card. The method preferably comprises the steps of connecting the smart card to an external host via a smart card reader electronic module and exchanging data with the smart card via the electronic module for contact mode of operation; and having an antenna assembly electrically coupling to said smart card and exchange data with a contactless smart card reader in a contactless mode of operation.

BRIEF DESCRIPTION OF FIGURES

FIG. 1 is a block diagram of a dual-mode smart card reader module according to the invention.

FIG. 2 is a dual-mode smart card whose dimension conforms to the SIM form factor.

FIG. 3 is top view of the dual-mode smart card reader device according to the invention with the top cover removed.

FIG. 4 is the top view of the dual-mode smart card reader device according to the invention with the dual-mode smart card inserted to the smart card connector slot of the device.

FIG. 5A, 5B, 5C and 5D are the first, second, third and forth layers of the printed circuit board layouts of the device according to the invention.

FIG. 6 is a cover of the device with an antenna embedded inside the cover.

FIG. 7 shows the printed circuit board installed on the cover of the device with an antenna embedded inside the cover.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention is now described in details hereinafter in the preferred embodiments. However, it will be obvious to one skilled in the art that the present invention may be practiced with variation of these specific details. Hence this invention should not be construed as limited to the embodiments set forth herein.

Referring to FIG. 1, the present invention is related to the dual-mode smart card reader module 10, which has two major components: the smart card reader electronic module 11 and the antenna assembly 12. The former establishes a communication path between the external host 21 and the smart card 20 so that the external host 21 can read and write information to the smart card 20 under the contact mode of operation. Likewise, the antenna assembly 12 provides the necessary antenna circuitry to smart card 20 so that the latter can communicate with the contactless smart card reader 22 in contactless mode of operation. In the preferred embodiment, the smart card 20 has a form factor like the SIM card as shown in FIG. 2, and the external host 21 is a computer. The smart card reader electronic module 11 provides a Universal Serial Bus (USB) port 31 for connection to the external host 21. However, it should be obvious to one skilled in the art that other interfacing protocols such as the RS232, the RS442 and the RS485 serial interface, as well as the parallel port interface can also be used. The antenna assembly 12 further comprises an antenna 14 and the antenna tuning circuitry 13. For certain dual-mode smart card, there is no need for antenna tuning and in this situation the antenna assembly 12 contains only the antenna 14.

FIG. 3 illustrates the entire apparatus of the preferred embodiment with the one part of the casing removed. The entire circuitry of the dual-mode smart card reader module 10 is implemented in the printed circuit board 33. In this preferred embodiment, the smart card reader module 10 makes use of the USB port 31 to connect to the external host 21. This module is housed in casing 32. The printed circuit board 33 contains a smart card connector 34 that has 8 pin connectors for making electrical contact with the dual-mode smart card 20. FIG. 4 shows the setting when the smart card 20 is inserted to the smart card connector 34.

FIG. 5 shows the entire layout of printed circuit board 33. In this preferred embodiment, the printed circuit board 34 has four layers. FIG. 5a and FIG. 5d are the top and bottom layers respectively for the mounting of discrete electronic components. The antenna 14 in FIG. 1 is realized in layer 2 and 3 of the printed circuit board 33. As shown in FIG. 5b and 5c, each of these two layers comprises five turns of thin electric wires that constitute a portion of the antenna. These wirings run around the perimeters of the printed circuit board so that the antenna 14 thus formed can capture the maximum amount of magnetic flux radiated from the contactless card reader 22. Thin wire 14a makes contact with layer 1 through electrically conducting pin-hole 15, and also with layer 3 through pin-hole 17. Likewise, thin wire 14b makes contact with layer 2 through pin-hole 17 and with layer 1 through pin-hole 16. As such, wiring 14a and 14b are connected together to form a single antenna 14. Antenna 14 connects to the antenna assembly 12 in printed circuit board 33, which in turn connects to smart card connector 34.

Since the electric power that can be coupled to the smart card 20 from the contactless smart card reader 22 depends on the number of turns that the loop antenna 14 has, and also the area it encloses, the wiring 14a and 14b preferably occupy the perimeter of the printed circuit board 33. To increase the number of turns, the loop antenna 14 occupies two layers of the printed circuit board in this specific embodiment,. Moreover, as surface mount technology is adopted to put electronic components to the printed circuit board 33, the top and bottom layers are dedicated to for interconnecting electronic components together to realize the circuitry of the dual-mode smart card reader module 10. Hence in the preferred embodiment, the loop antenna 14 occupies the inner two layers. If there is no size constrain, the antenna can be co-located with the rest of the electronic circuitry and hence the number of layers in the printed circuit board 33 can be reduced. Although the present invention has been described specifically using this preferred embodiment, it is clear that many variations and combinations are possible in the light of the teaching provided herein. Specifically, the number of turns of the antenna wiring, its placement on the circuit board, and the number of layers of the printed circuit board used are variations that those skilled in the technical art can adapt to their specific applications.

In another preferred embodiment, the antenna 14 is embedded in the casing 32 as shown in FIG. 6. The antenna can be constructed using thin metal wires wound in loops or other forms, or it can be printed onto the cover using conductive inks. The main purpose is that the antenna thus formed can receive the electromagnetic wave radiated from the contactless card reader. At the printed circuit board 33, spring connectors can be placed directly underneath antenna leads 41 and 42, so that when the cover 32 encloses the printed circuit board 33, these spring connectors make electrical connections to antenna leads 41 and 42. In another preferred embodiment, flexible circuit board can be used to form the antenna 14, and the former can be glued to the back of the cover 32 by adhesive means. The antenna 14 can be connected to the printed circuit board 33 through ordinary electrical wires and connectors. It should be obvious to one skilled in the art that there can be a plurality of methods to embed the antenna 14 to the cover 32 and connect the antenna to the printed circuit board 33; and the antenna can be made using a variety of electrically conducting materials. The preferred embodiment describes herein represents only one approach to reduce the inventive idea to practice. Many other alternatives and variations may be made from the teaching above.

The preferred embodiments of the present invention are thus fully described. Although the description referred to particular embodiments, it should not be construed that the invention is limited to such embodiments, but rather construed according to the claims below.

What is claimed is:

1. An apparatus for reading a dual-mode smart card comprising
   a. a smart card connector adapted to electrically connect to said smart card;
   b. a smart card reader electronic module connecting said smart card connector to an external port, said external port adapted for electrically coupling to an external host for data exchange between said smart card and said external host;
   c. an antenna assembly adapted to electrically connect to said smart card connector for wireless data transmission between said smart card and a contactless smart card reader.
2. An apparatus according to claim 1, wherein said smart card connector is fabricated on a printed circuit board.
3. An apparatus according to claim 2, wherein said antenna assembly is fabricated in said printed circuit board.
4. An apparatus according to claim 3, wherein said printed circuit board is a multi-layer printed circuit board with at least one layer of said printed circuit board containing at least a portion of said antenna assembly.
5. An apparatus according to claim 4 wherein said printed circuit board further comprises multiple layers said antenna assembly being embedded in at least two layers of said printed circuit board with electrically conduction therebetween.
6. An apparatus as in claim 1 or 2, wherein a casing is provided for housing at least a portion of said apparatus, and the antenna of said antenna assembly is embedded as part of said casing.
7. An apparatus as in claim 1, wherein said external port is a USB port.
8. An apparatus as in claim 1, wherein said external port is a serial port.
9. In a smart card reading apparatus containing a smart card reader electronic module for connecting an export port to a smart card connector, said smart card connector adapted to electrically connect to a dual-mode smart card, said smart card electrically coupling to an antenna assembly for contactless mode of operation, a method of forming said antenna assembly comprising the steps of
   a. laying metal conductors in a printed circuit board to connect

i. electronic components of said export port,

ii. said smart card reader electronic module, and

iii. said smart card connector together.

b. embedding at least one metal wire in a position proximate the perimeter of said printed circuit board;

c. electrically connecting said metal wire to said smart card connector such that said metal wire functions as an antenna for said antenna assembly for wireless transmission.

10. A method according to claim 9 further comprising embedding at least a second metal wire in at least a second layer; and connecting said first metal wire with said second wire electrically.

11. A method according to claim 10 wherein said metal wire is embedded in the inner layers of said multiple layer printed circuit board.

12. A method of accessing a dual-mode smart card comprising the steps of connecting said smart card to an external host via a smart card reader electronic module and transferring data to and from said smart card via said electronic module for contact mode of operation; and having an antenna assembly electrically coupling to said smart card and transferring data to and from said smart card for contactless mode of operation.

13. A method according to claim 12 further comprising providing a casing to house said printed circuit board; winding an electrically conducting wire around said casing in multiple turns; and connecting said wire to said antenna assembly in said printed circuit board.

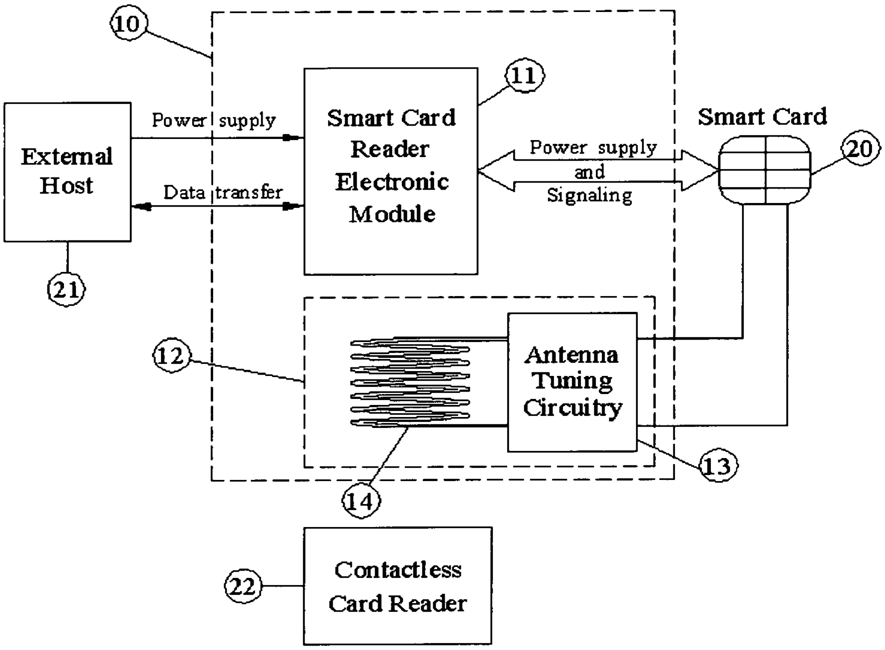

10
11
External
Host
Power supply
Data transfer
Smart Card
Reader
Electronic
Module
Power supply
and
Signaling
Smart Card
20
21
12
Antenna
Tuning
Circuitry
13
14
22
Contactless
Card Reader

FIG.1

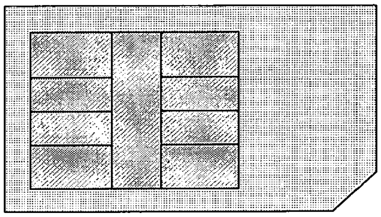


FIG. 2

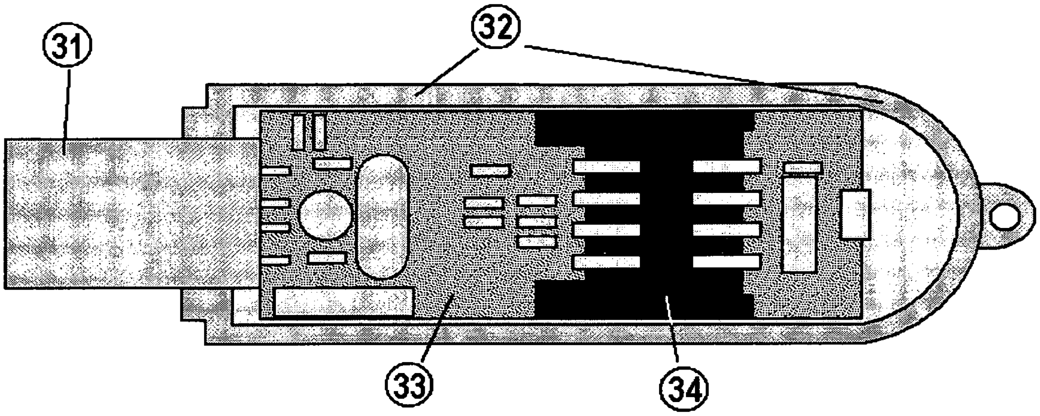


FIG.3

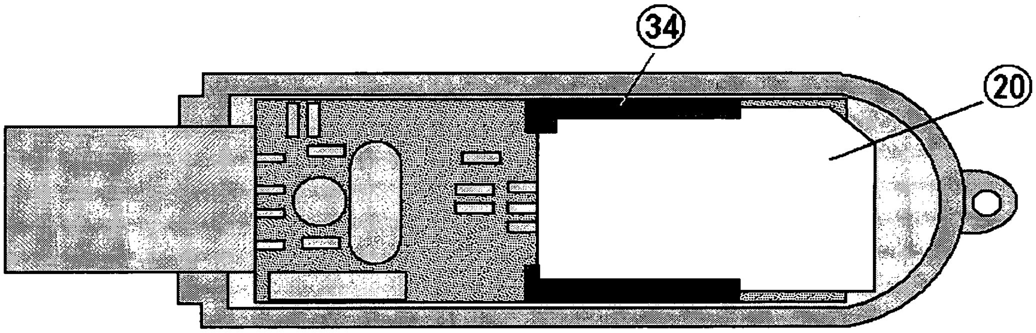


FIG.4

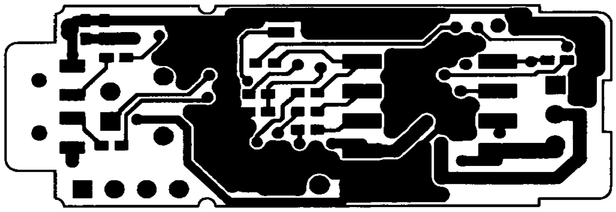


FIG. 5A

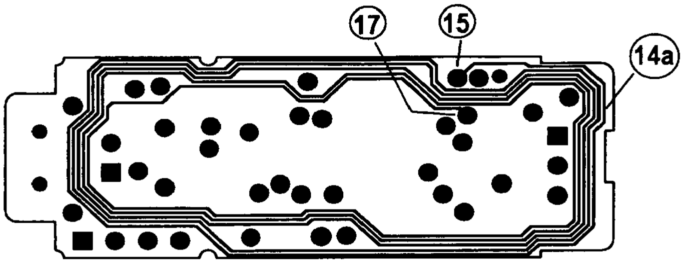


FIG. 5B

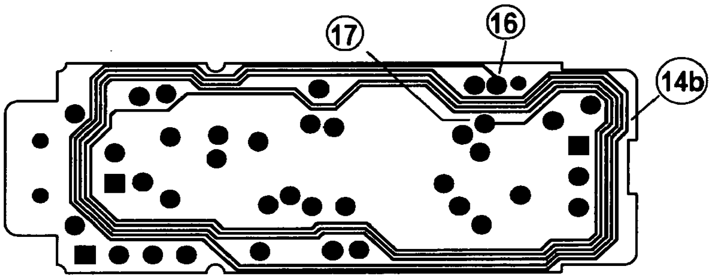


FIG. 5C

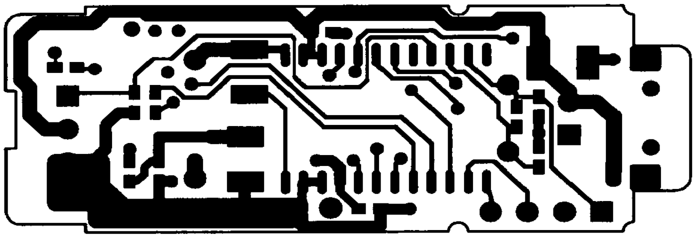


FIG. 5D

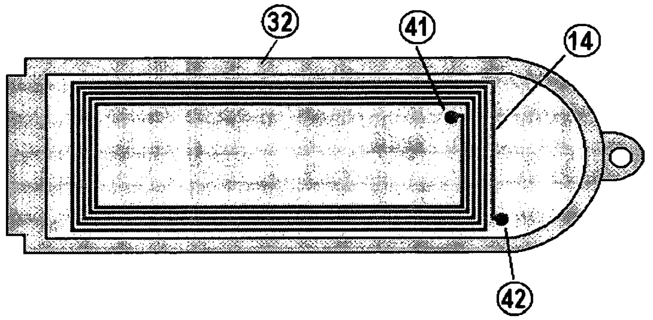


FIG. 6

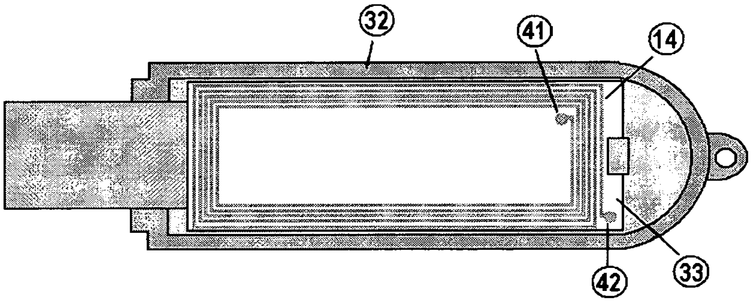


FIG. 7

TITLE

A SMART CARD RELEASING MECHANISM FOR SMART CARD READER

FIELD OF INVENTION

This invention relates to an electronic apparatus, and in particular a smart-card reader that possesses a quick release mechanism for users to retrieve the inserted smart card easily.

BACKGROUND OF INVENTION

Smart IC cards have been widely used in many applications. It consists of an IC chip embedded in a flat enclosure and typically comes with two types of form factors. One of them is the size of a normal credit card. The other is a smaller Subscriber Identification Module (SIM) widely used in mobile phones and is generally referred to as SIM card. A smart card reader is a device that provides a communication path for the host computer to access the content of the smart card. There are smart card readers specially made for the SIM card. Since the SIM card is small enough, the corresponding reader can be made in a size that is handy to carry. It can be used as a secured token for logging on to computer systems or conducting e-commerce transactions. In another application, such a reader can be used to upload the information stored in the SIM card of a mobile phone to a host computer database.

However, it is not easy to remove the SIM card from the reader in existing products. The user typically needs to take a portion of the device's cover away first, and then use his finger to slide the SIM card away from the smart card connector within the device. It is therefore very inconvenient for the user if he needs to access the contents of many SIM cards in a short time. The present invention describes a quick-release mechanism that can be easily incorporated to a smart card reader so that the user can retrieve the smart card at ease.

SUMMARY OF INVENTION

In view of the background discussion, it is an object of this invention to provide an easy-to-use smart card dispensing mechanism to eject the smart card from a smart card reader apparatus. Accordingly, the present invention relates to an apparatus comprising a housing, a printed circuit board fitted inside the housing with a receiving site to accommodate a smart card, and a smart card dispensing module disposed in between the housing and the printed circuit board. One side of the dispensing module is at least partially exposed to the exterior of the housing while the other side makes mechanical contact to the smart card when the latter is inserted to the apparatus. The first side is adapted to receive a user triggering movement that causes the dispensing module to eject the smart card from the receiving site.

In a preferred embodiment, the housing of the apparatus comprises first and second covers, with an opening on the second cover. One side of the dispensing module comprises a first protruded element that fits to the opening of the second cover for the user to apply his triggering movement. The other side of the dispensing module comprises a second protruded element that makes contact to the smart card when the latter is inserted to the apparatus. In the preferred embodiment, the insertion of the smart card pushes the dispensing module to a first position inside the apparatus. When the user applies a triggering movement onto the first protruding element of the dispensing module, it causes the dispensing module to slide to a second position and eject the smart card from the receiving site.

In the present preferred embodiment, the first protruded element of the dispensing module has at least one groove to facilitate the user to apply his triggering movement. Furthermore, the opening of the second cover has a wider opening at the exterior side compared to the interior side. In addition, the dispensing module further comprises an elongated arm in one sliding direction and a knot at the end of the elongated arm.

Correspondingly, the interior side of the second cover further comprises at least 2 notches so that the knob can rest on one of these notches securely.

The method aspect of the present invention is related to a user-friendly process to release a smart card from the above-described device in its broadest embodiment. The method comprises the steps of pushing the dispensing module to a first position when the smart card is inserted to the device, and ejecting the smart card from the receiving site when the user applies the triggering movement to the first protruding element of the dispensing module, forcing the latter to slide to the second sliding position.

BRIEF DESCRIPTION OF FIGURES

FIG. 1 is the top view of the interior of smart card reader device according to the invention with the second cover removed.

FIG. 2 is a smart card whose dimension conforms to the SIM form factor.

FIG. 3 is the top view of the smart card reader device according to the invention with the smart card inserted into the receiving site of the device.

FIG 4A and 4B are the top view and side view of the first cover that houses the device.

FIG 5A and 5B are the top view and side view of the second cover that houses the device.

FIG. 6A, 6B and 6C are the perspective view, top view and side view of the dispensing module.

FIG. 7A and 7B are the cross-section side views of the apparatus showing respectively the first position of the dispensing module when the smart card is inserted into the device and the second position when it is pushed by the user to eject the smart card.

FIG. 8A and 8B illustrate the beveled edge of the opening of the second cover and its relative positioning against the dispensing module.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

The present invention is now described in details hereinafter in the preferred embodiments. However, it will be obvious to one skilled in the art that the present invention may be practiced with variation of these specific details. Hence this invention should not be construed as limited to the embodiments set forth herein.

FIG. 1 shows a printed circuit board 20 fitted inside the first cover 11. The printed circuit board 20 connects the electronic components soldered in it to implement the smart card controller logic. One of the components is the receiving site 21 specially made to house the SIM card. FIG. 2 depicts the smart card 22 in SIM form factor. The printed circuit board 20 also connects to a Universal Serial Bus (USB) connector 23 that serves as a mean to communicate to the host computer. However, it should be obvious to one skilled in the art that other interfacing protocols such as the RS232, RS485, or RS422 serial protocol and other parallel interfaces can also be adopted. FIG. 3 shows the apparatus with the smart card 22 inserted into the receiving site 21 thereof. FIG. 4A and 4B are the top and side views of the first cover 11 of the housing, whilst FIG. 5A and 5B are the top and side views of the second cover 30 respectively. Both the first and second covers 11 and 30 respectively have recesses 12 and 34 at the front so that when the first cover 11 are placed on top of the second cover 30, an open space at the front of the apparatus is formed so that the smart card 22 can slide in. The second cover has an opening 31 and also a plurality of notches 32 as shown in FIG. 5A. FIG. 6A, 6B and 6C are the perspective, top and side views of the dispensing module 40 that is fitted in between the second cover 30 and the printed circuit board 20. The dispensing module 40 comprises a first protruding element 43 that is fitted to the opening 31 of the second cover 30. It also comprises a second protruding element 45 on the other surface of the dispensing module 40, and an elongated arm 41. The end of the elongated arm 41 comprises a knob 42. The dispensing module 40 can slide inside the apparatus with little restriction. FIG. 7A indicates a cross section view of the apparatus when smart card 22 is inserted. Specifically, when the smart card 22 is being inserted, it makes contact to the second protruding element of the dispensing module 45, and pushes the dispensing module 40 to a first position inside the apparatus. When the smart card 22 is fully inserted, it sits on the receiving site 21 which has electrical contacts that connect to the respective contacts of the smart card 22.

To release the smart card 22 from the apparatus, a user can apply a triggering movement by placing his finger on the first protruding element 43 of the dispensing module 40, and exert a force to push it outward to a second position. As a result, the smart card 22 is disengaged from the receiving site 21 and is partially exposed outside the apparatus as shown in FIG. 7B so that it can be retrieved by the user easily.

In the preferred embodiment, the first protruding element 43 of the dispensing module 40 further comprises a plurality of grooves 44 to facilitate the user to securely place his fingers onto the dispensing module 40 and to exert force. Moreover, the second cover 30 comprises a plurality of notches 32 so that knob 42 can rest on one of these notches 32. This will prevent the dispensing module 40 to slide freely inside the apparatus and causes it to either rest on a first position or a second position as mentioned earlier.

Yet another invention in the present preferred embodiment is related to the shape of the opening 31 of the second cover 30 as shown in FIG. 8A. The opening 31 comprises a beveled edge 35 that is wider in the exterior side compared to the interior side 36. When the first protruding element 43 is fitted to the opening 31 as shown in FIG. 8B, the top of the first protruding element 43 of the dispensing module 40 needs not be higher than the second cover 30 to cause unevenness when the apparatus is placed on a flat surface, yet the beveled edge 35 allows the user's finger to get deeper into the opening 31 so that the finger can make a firmer contact with the first protruding element 43.

The preferred embodiments of the present invention are thus fully described. Although the description referred to specific embodiments, it should be understood that the invention is not limited to such embodiments, but rather construed according to the claims below.

What is claimed is:

1. A smart card reader apparatus comprising:
   a. a housing
   b. a printed circuit board disposed within said housing and implementing a smart card reader module, said printed circuit board further comprising a receiving site adapted to receive a smart card,
   c. a smart card dispensing module disposed within said housing, said smart card dispensing module further having a first side at least partially exposed to the exterior of said housing and adapted to receive user instruction and a second side adapted to mechanically couple to said smart card such that a triggering movement of the user on said first side of said dispensing module can cause said dispensing module to eject said smart card from said receiving site.
2. An apparatus according to claim 1 wherein said housing comprising a first cover and a second cover, said second cover further comprising an opening for exterior access of said first side of said smart card disposing module by said user.
3. An apparatus according to claim 2 wherein said opening of said second cover further comprising an exterior side and an interior side, said exterior side having a beveled edge with outer perimeter wider than the inner perimeter to allow easy access.
4. An apparatus according to claim 2 wherein said dispensing module is dispose between said housing and said printed circuit board, said dispensing module further adapted to slide to a first position when said smart card is inserted in said receiving site and to a second position when said user exerts said triggering movement.
5. An apparatus according to claim 4 wherein said first side of said dispensing module further comprising a first protruded element extending through said opening of said second cover adapted for receiving said triggering movement of said user.
6. An apparatus according to claim 4 wherein said second side of said dispensing module further comprising a second protruded element adapted to establish mechanical contact with said smart card when it is inserted to said apparatus.

7. An apparatus according to claim 5 wherein said first protruded element of said dispensing module has at least one groove to facilitate said user to exert said triggering movement.
8. An apparatus according to claim 2 wherein said dispensing module further comprising an elongated arm in one sliding direction and a knob at the end of said elongated arm.
9. An apparatus according to claim 8 wherein the interior of second cover further comprising at least 2 notches so that said knob of said elongated arm of said dispensing module rests on one of said notches of said second cover securely.
10. A method of ejecting a smart card from an apparatus that comprises a housing, a printed circuit board that houses a smart card receiving site, a first cover of said housing, a second cover with an opening, a dispensing module disposed in between said printed circuit board and said second cover, a first protruding element in one surface of said dispensing module fitted to said opening of said second cover and a second protruding element in the opposite surface of said dispensing module comprising:
    a. pushing said dispensing module to a first sliding position when said smart card is inserted and fitted onto said smart card receiving site,
    b. ejecting said smart card from said receiving site when said user applies said triggering movement onto said first protruding element of said dispensing module causing said dispensing module to slide to said second sliding position.

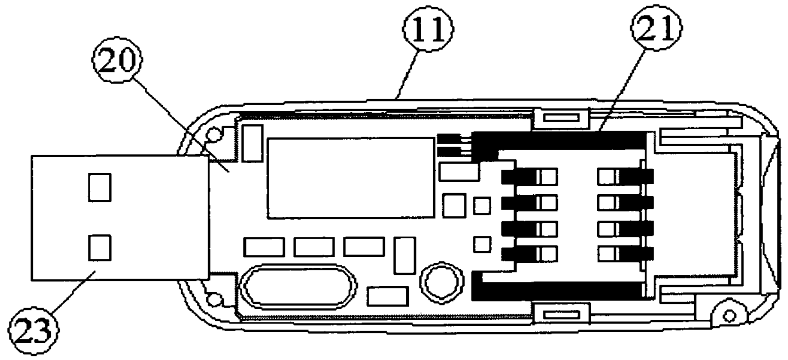


FIG. 1

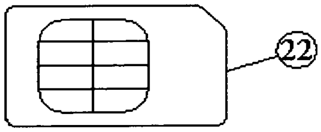


FIG. 2

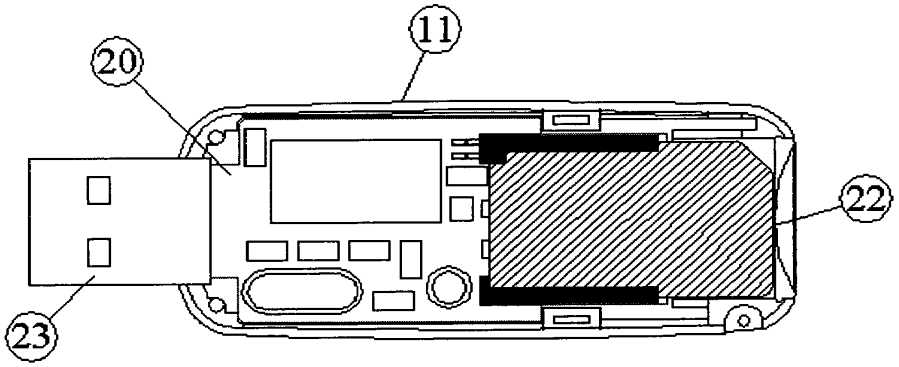


FIG. 3

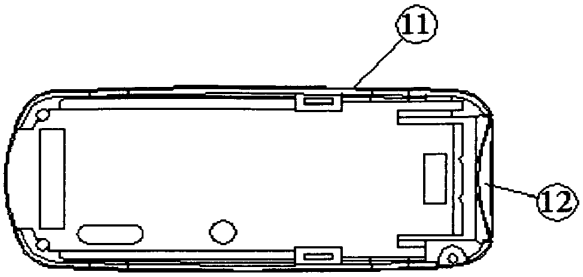


FIG. 4A

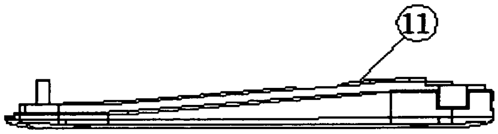


FIG. 4B

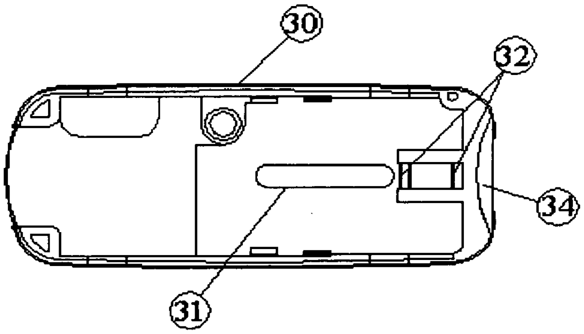


FIG. 5A

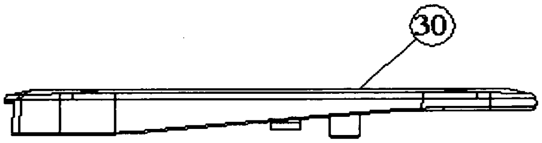


FIG. 5B

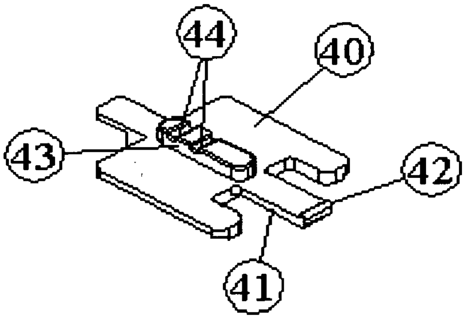


FIG. 6A

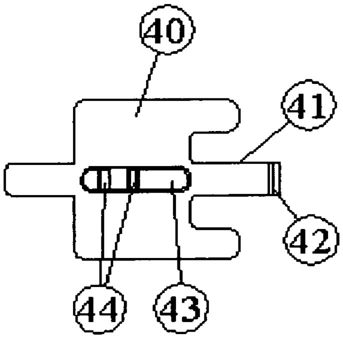


FIG. 6B

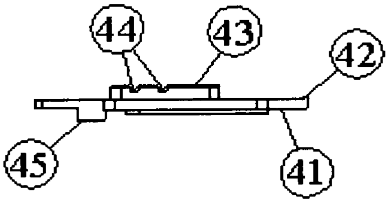


FIG. 6C

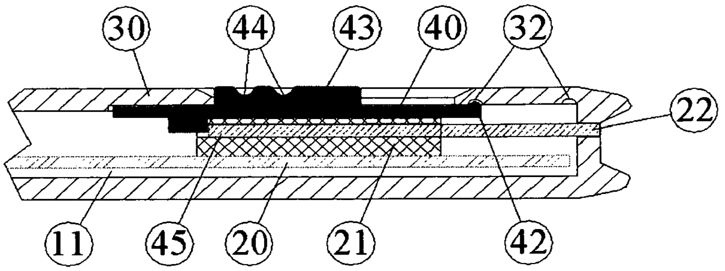


FIG. 7A

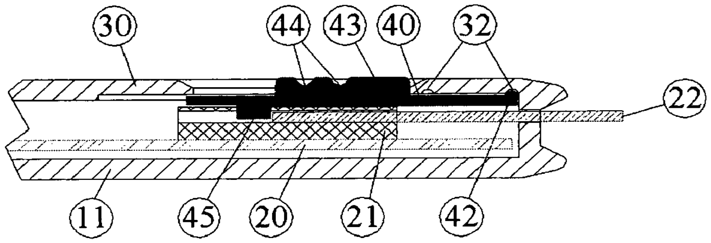


FIG. 7B

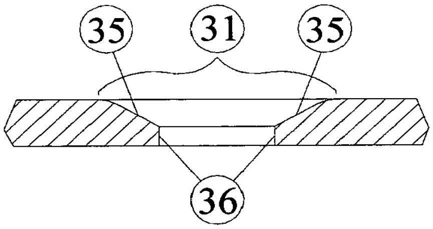


FIG. 8A

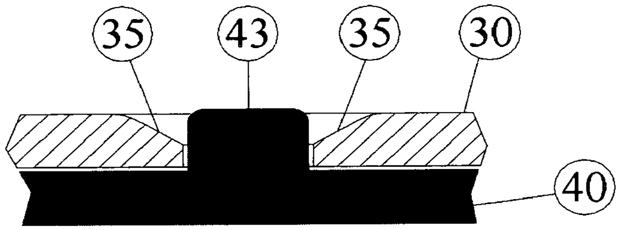


FIG. 8B

(19) **日本国特許庁(JP)**

(12) **公 開 特 許 公 報(A)**

(11) 特許出願公開番号

特開2004-246720

(P2004-246720A)

(43) 公開日 **平成16年9月2日(2004. 9. 2)**

(51) Int.Cl.⁷	F I			テーマコード（参考）
G06F 9/445	G06F	9/06	610A	5B014
G06F 1/00	G06F	13/10	330B	5B076
G06F 13/10	G06F	15/00	330B	5B085
G06F 15/00	G06F	15/00	390	
	G06F	9/06	610L	

審査請求 未請求　請求項の数 5　ＯＬ　（全 23 頁）　最終頁に続く

(21) 出願番号　特願2003-37225 (P2003-37225)

(22) 出願日　平成15年2月14日 (2003. 2. 14)

(71) 出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中４丁目１番１号

(74) 代理人　100079359
弁理士　竹内　進

(72) 発明者　佐沢　真一
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(72) 発明者　佐藤　裕一
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

(72) 発明者　千田　陽介
神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

最終頁に続く

(54) 【発明の名称】 情報処理デバイス、情報処理方法及びプログラム

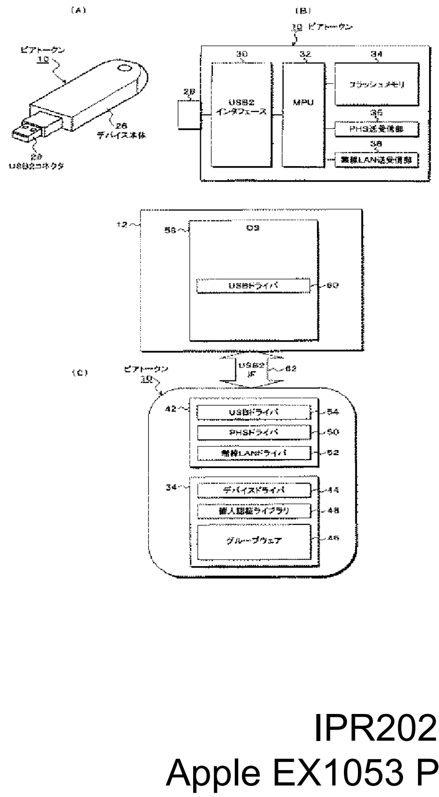
(57)【要約】

【課題】任意のパーソナルコンピュータに個人認証を必要とするグループウェア等の個人の作業環境を簡単に構築して利用可能とする。

【解決手段】ピアトークン１０と呼ばれる情報処理デバイスは、電源供給とデータ転送が可能なパーソナルコンピュータ１２のデバイスポートに対し着脱自在なポートコネクタと、外部装置に対し無線回線により情報を送受する第１無線通信部と、外部装置に対し第１無線通信部とは異なる無線回線を使用して情報を送受する第２無線通信部と、デバイスドライバ４４、ＵＳＢドライバ５４、個人認証ライブラリ４８、グループウェア４６、第１無線通信用ドライバ及び第２無線通信用ドライバを格納した不揮発メモリ３４をもつ。ピアトークン１０をパーソナルコンピュータ１２のデバイスポートに接続すると、デバイスドライバのインストール、個人認証ライブラリのインストールによる個人認証を経てアプリケーションプログラムをインストールして実行させる。

【選択図】　図１

本発明の原理説明図



【特許請求の範囲】

【請求項1】

電源供給とデータ転送が可能な情報処理装置のデバイスポートに対し着脱自在なポートコネクタと、

外部装置に対し無線回線により情報を送受する第１無線通信部と、

外部装置に対し前記第１無線通信部とは異なる無線回線を使用して情報を送受する第２無線通信部と、

デバイスドライバ、ポートドライバ、個人認証ライブラリ、任意のアプリケーションプログラム、第１無線通信用ドライバ及び第２無線通信用ドライバを格納した不揮発メモリと、

前記ポートコネクタを情報処理装置のデバイスポートに接続した際に起動し、前記情報端末装置からの最初のデバイスアクセスに対し前記デバイスドライバを転送してインストールさせ、インストールされた前記デバイスドライバにより前記個人認証ライブラリをインストールさせて個人認証を行わせ、個人認証に成功した場合に前記アプリケーションプログラムをインストールして実行させ、前記認証ライブラリ及びアプリケーションプログラムの実行による外部装置とのアクセスを前記第１又は第２無線通信用ドライバにより行わせ、アプリケーションの終了時には前記デバイスドライバ、個人認証ライブラリ及びアプリケーションプログラムをアンインストールさせるデバイス処理部と、

を備えたことを特徴とする情報処理デバイス。

【請求項2】

請求項１記載の情報処理デバイスに於いて、前記アプリケーションプログラムは複数の情報処理装置でデータを共有するピアツーピア型のグループウェア処理プログラムであることを特徴とする情報処理デバイス。

【請求項3】

請求項１記載の情報処理デバイスに於いて、前記不揮発メモリに自己の情報処理装置で使用しているファイルをサーバに格納したことを示すディレクトリ情報を登録し、前記アプリケーションプログラムは、他の情報処理装置の差込み時に、前記レジストリ情報により前記サーバからファイルを取得して前記自己の情報処理装置の作業環境を構築することを特徴とする情報処理デバイス。

【請求項4】

電源供給とデータ転送が可能な情報処理装置のデバイスポートに対し着脱自在なポートコネクタと、外部装置に対し無線回線により情報を送受する第１無線通信部と、外部装置に対し前記第１無線通信部とは異なる無線回線を使用して情報を送受する第２無線通信部と、デバイスドライバ、ポートドライバ、個人認証ライブラリ、任意のアプリケーションプログラム、第１無線通信用ドライバ及び第２無線通信用ドライバを格納した不揮発メモリとを備えた情報処理デバイスの情報処理方法に於いて、

前記ポートコネクタを情報処理装置のデバイスポートに接続した際に起動し、前記情報端末装置からの最初のデバイスアクセスに対し前記デバイスドライバを転送してインストールさせる起動ステップと、

インストールされた前記デバイスドライバにより前記個人認証ライブラリをインストールさせて個人認証を行わせる個人認証ステップと、

個人認証に成功した場合に前記アプリケーションプログラムをインストールして実行させる実行ステップと、

前記認証ライブラリ及びアプリケーションプログラムの実行による外部装置とのアクセスを前記第１又は第２無線通信用ドライバにより行わせる通信ステップと、

アプリケーションプログラムの終了時に前記デバイスドライバ、個人認証ライブラリ及びアプリケーションプログラムをアンインストールさせるアンインストールステップと、

を備えたことを特徴とする情報処理方法。

【請求項5】

電源供給とデータ転送が可能な情報処理装置のデバイスポートに対し着脱自在なポートコ

ネクタと、外部装置に対し無線回線により情報を送受する第１無線通信部と、外部装置に対し前記第１無線通信部とは異なる無線回線を使用して情報を送受する第２無線通信部と、デバイスドライバ、ポートドライバ、個人認証ライブラリ、任意のアプリケーションプログラム、第１無線通信用ドライバ及び第２無線通信用ドライバを格納した不揮発メモリとを備えた情報処理デバイスのコンピュータに、

前記ポートコネクタを情報処理装置のデバイスポートに接続した際に起動し、前記情報端末装置からの最初のデバイスアクセスに対し前記デバイスドライバを転送してインストールさせる起動ステップと、

インストールされた前記デバイスドライバにより前記個人認証ライブラリをインストールさせて個人認証を行わせる認証ステップと、

個人認証に成功した場合に前記アプリケーションプログラムをインストールして実行させる実行ステップと、

前記認証ライブラリ及びアプリケーションプログラムの実行による外部装置とのアクセスを前記第１又は第２無線通信用ドライバにより行わせる通信ステップと、

アプリケーションプログラムの終了時に前記デバイスドライバ、個人認証ライブラリ及びアプリケーションプログラムをアンインストールさせるアンインストールステップと、

を実行させることを特徴とするプログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、任意のパーソナルコンピュータに対し個人のコンピュータ環境を構築する携帯型の情報処理デバイス、情報処理方法及びプログラムに関し、特に、ピアツーピア型のグループウェアのコンピュータ環境を簡単に構築する情報処理デバイス、情報処理方法及びプログラムに関する。

【０００２】

【従来の技術】

従来、自分のパーソナルコンピュータと同じ環境を出張などの外出先で実現する方法としては、ラップトップやＰＤＡといった携帯型のデバイスに個別に自己の作業環境を構築しておき、事前に作業に必要なデータを日常的に使用しているデスクトップ等からメールの添付や無線回線などを利用して転送し、これを持ち運んで使用している。

【０００３】

また出張先によっては、そこに設置しているデスクトップ等を自由に使用できる場合があることから、文書入力といった汎用的なアプリケーションで足りる場合には、パーソナルコンピュータを借用して作業することができる。

【０００４】

【特許文献１】

販売元株式会社サクセス、製造元エニワン株式会社、“ＵＳＢストレージ［ビー・エニィウェアー］”、［平成１５年２月３日検索］、インターネット＜ＵＲＬ　：　ＨＹＰＥＲＬＩＮＫ ｈｔｔｐ：／／ｂｅｅｍａｉｌ．ｊｐ／ａｎｙｗｈｅｒｅ．ｈｔｍｌ ＵＲＬ：／／ｗｗｗ．ｂｅｅｍａｌ．ｊｐ／／ａｎｙｗｈｅｒｅ．ｈｔｍｌ＞

【０００５】

【発明が解決しようとする課題】

しかしながら、パーソナルコンピュータの環境は、デスクトップやラップトップといったパーソナルコンピュータ毎に固有な場合がほとんどであり、例えば、メールの場合、事務所等に設置して使用しているデスクトップと出張に持ち歩くラップトップとでは、アドレス帳などの環境や受信メール本体に常に差分が生じてしまい、非常に不便な状況が発生している。

【０００６】

このような問題を解決するため、例えばウェブメールやＩＭＡＰ４等のプロトコルによるサーバによる一元管理の方法もあるが、一元管理に伴う個人毎の容量制限やクライアント

・サーバモデルによる反応速度の低下といった問題がある。

【０００７】

また持ち歩いているラップトップにつき、無線ＬＡＮやＰＨＳを使ってメール等を通信する場合、それぞれ専用のパーソナルコンピュータ向けのＭＣＩＡカードが必要であり、場合によってはパーソナルコンピュータ毎にドライバソフトのインストールし、必要な設定作業を行うといった面倒な作業が要求される。

【０００８】

更に、サーバ等にアクセスしてデータを利用する場合、通常、ＩＤとパスワードを入力する個人認証を必要とし、そのため出張時にラップトップを使用する場合にも煩雑な認証操作が必要となる。この問題を解消するものとしてＵＳＢトークンまたはＩＣカードによる個人認証デバイスが存在する。しかし、これらの個人認証デバイスは、個人認証を行う機能に限られており、個人のコンピュータ環境の構築には対応していない。

【０００９】

一方、メモリステックのようにメモリのみを内蔵したカードやトークンも存在するが、これらは単なるメモリ機能しか持たず、個人のコンピュータ環境の構築には対応していない。

【００１０】

更にＵＳＢの内部にメールソフトを予めインストールしたデバイスも存在するが（特許文献１）、用途がメールに限られており、認証を含む汎用的なアプリケーションに対応したコンピュータ環境の構築には対応できない。

【００１１】

本発明は、任意のパーソナルコンピュータに個人認証を必要とするグループウェア等の個人の作業環境を簡単に構築して利用できる情報処理デバイス、情報処理方法及びプログラムを提供することを目的とする。

【００１２】

【課題を解決するための手段】

図１（Ａ）（Ｂ）（Ｃ）は本発明の原理説明図である。本発明の情報処理デバイス（ピアトークン１０）は、電源供給とデータ転送が可能な情報処理装置のデバイスポートに対し着脱自在なポートコネクタと、外部装置に対し無線回線により情報を送受する第１無線通信部（ＰＨＳ送受信部３６）と、外部装置に対し第１無線通信部とは異なる無線回線を使用して情報を送受する第２無線通信部（無線ＬＡＮ送受信部３８）と、デバイスドライバ４４、ポートドライバ、個人認証ライブラリ４８、任意のアプリケーションプログラム、第１無線通信用ドライバ及び第２無線通信用ドライバを格納した不揮発メモリ（フラッシュメモリ３４）と、ポートコネクタを情報処理装置（パーソナルコンピュータ１２）のデバイスポートに接続した際に起動し、情報端末装置からの最初のデバイスアクセスに対しデバイスドライバを転送してインストールさせ、インストールされたデバイスドライバにより個人認証ライブラリをインストールさせて個人認証を行わせ、個人認証に成功した場合にアプリケーションプログラムをインストールして実行させ、認証ライブラリ及びアプリケーションプログラムの実行による外部装置とのアクセスを第１又は第２無線通信用ドライバにより行わせ、アプリケーションの終了時には前記デバイスドライバ、個人認証ライブラリ及びアプリケーションプログラムをアンインストールさせるデバイス処理部とを備えたことを特徴とする。

【００１３】

このため本発明は、情報処理デバイスを任意のパーソナルコンピュータやＰＤＡ等のデバイスポートに差し込むだけで、個人認証画面が自動的に立ち上がり、個人認証を済ませた後は、グループウェア等のアプリケーション画面が立ち上がり、外部との送受信を含む作業をすぐ始めることができる。

【００１４】

また無線通信機能が二重化されており、使用場所の無線環境に合わせて自動切換えして外部装置に確実にアクセスできる。

【００１５】
更にアプリケーションの実行で使用されたデータは全て不揮発メモリに保存され、また本発明のデバイスを抜いて処理を終えると、パーソナルコンピュータにインストールしたプログラムやドライバは全てアンインストールされ、本発明のデバイスを差し込んで使用したパーソナルコンピュータ本体の環境をまったく侵蝕することがない。

【００１６】
ここでデバイス本体２６は持ち運び自在なキー型である。またデバイスポートは例えばＵＳＢ２コネクタ２８であり、ポートドライバはＵＳＢドライバ５４である。更に第１無線通信部はＰＨＳ無線回線を使用するＰＨＳ送受信部３６であり、第２無線通信部は無線ＬＡＮを使用する無線ＬＡＮ送受信部３８である。

【００１７】
本発明の情報処理デバイスによりインストールするアプリケーションプログラムは、複数の情報処理装置でデータを共有するピアツーピア型のグループウェア４６の処理プログラムである。

【００１８】
このようにアプリケーションプログラムがグループウェア処理プログラムの場合、個人認証ライブラリは第１又は第２無線通信部により外部の認証サーバに接続して認証処理を実行させせる。

【００１９】
グループウェア処理プログラムは、不揮発メモリに共有データを保持し、起動時にグループウェアに属している他の情報処理装置の保持している共有データとの同期をとる。即ち、グループウェア処理プログラムは、自己の共有データと他の情報処理装置との非同期を検知した場合、他の装置から差分データを受信してマージすることにより共有データの同期をとる。このため出張先のコンピュータを使用する際にも、最新の共有データを利用できる。

【００２０】
グループウェア処理プログラムは、使用済みファイルを不揮発メモリに格納する際にメモリ容量の不足を検知した場合、ファイルリストの末尾に格納しているファイルをグループウェアに属する他の情報処理装置に転送した後にファイルを消去して保存先のリンク情報を格納し、その後に使用済みファイルをファイルリストの先頭位置に格納する。

【００２１】
このためデバイス内蔵メモリに制約があっても、グループウェアに属する例えば近隣のピア装置となるパーソナルコンピュータに共有データを転送保持させ、そのリンク情報のみをデバイス内に保持することで、メモリ容量に制限があっても共有データを確実に保存できる。このデバイスの不揮発性メモリに保持したリンク情報は、自分のパーソナルコンピュータを使用する際に、本発明のデバイスを差し込むことによりリンク情報で指定される保存先から実データを取得して保持することができる。

【００２２】
また情報処理デバイスにあっては、不揮発メモリに自己の情報処理装置で使用しているファイルをサーバに格納したことを示すレジストリ情報を登録し、アプリケーションプログラムは、他の情報処理装置の差込み時に、不揮発メモリに登録しているレジストリ情報によりサーバからファイルを取得して自己の処理装置の作業環境を構築する。

【００２３】
本発明の別の形態にあっては、情報処理デバイスのポートコネクタにより接続する情報処理装置は携帯電話であり、この場合、アプリケーションプログラムは、交通機関の改札ゲートの通過時にゲート開制御と課金処理を行うことを特徴とする。また情報処理デバイスのポートコネクタにより接続する情報処理装置は携帯電話であり、アプリケーションプログラムは、自動販売機との間で商品の購入処理を行うことを特徴とする。このように交通機関の改札や自動販売機の利用につき、無線機能を利用した処理が簡単にできる。

【００２４】

本発明は任意のパーソナルコンピュータにグループウェア等の個人の作業環境を簡単に構築して利用できる情報処理方法を提供する。

【００２５】

即ち、本発明は、電源供給とデータ転送が可能な情報処理装置のデバイスポートに対し着脱自在なポートコネクタと、外部装置に対し無線回線により情報を送受する第１無線通信部と、外部装置に対し第１無線通信部とは異なる無線回線を使用して情報を送受する第２無線通信部と、デバイスドライバ、ポートドライバ、個人認証ライブラリ、任意のアプリケーションプログラム、第１無線通信用ドライバ及び第２無線通信用ドライバを格納した不揮発メモリとを備えたデバイスの情報処理方法であって、

ポートコネクタを情報処理装置のデバイスポートに接続した際に起動し、情報端末装置からの最初のデバイスアクセスに対しデバイスドライバを転送してインストールさせる起動ステップと、

インストールされたデバイスドライバにより個人認証ライブラリをインストールさせて個人認証を行わせる認証ステップと、

個人認証に成功した場合にアプリケーションプログラムをインストールして実行させる実行ステップと、

認証ライブラリ及びアプリケーションプログラムの実行による外部装置とのアクセスを第１又は第２無線通信用ドライバにより行わせる通信ステップと、

アプリケーションプログラムの終了時にデバイスドライバ、個人認証ライブラリ及びアプリケーションプログラムをアンインストールさせるアンインストールステップと、

を備えたことを特徴とする。

【００２６】

本発明は、任意のパーソナルコンピュータにグループウェア等の個人の作業環境を簡単に構築して利用できるコンピュータで実行されるプログラムを提供する。

【００２７】

即ち、本発明のプログラムは、電源供給とデータ転送が可能な情報処理装置のデバイスポートに対し着脱自在なポートコネクタと、外部装置に対し無線回線により情報を送受する第１無線通信部と、外部装置に対し第１無線通信部とは異なる無線回線を使用して情報を送受する第２無線通信部と、デバイスドライバ、ポートドライバ、個人認証ライブラリ、任意のアプリケーションプログラム、第１無線通信用ドライバ及び第２無線通信用ドライバを格納した不揮発メモリとを備えた情報処理デバイスのコンピュータに、

ポートコネクタを情報処理装置のデバイスポートに接続した際に起動し、情報端末装置からの最初のデバイスアクセスに対しデバイスドライバを転送してインストールさせる起動ステップと、

インストールされた前記デバイスドライバにより個人認証ライブラリをインストールさせて個人認証を行わせる認証ステップと、

個人認証に成功した場合にアプリケーションプログラムをインストールして実行させる実行ステップと、

認証ライブラリ及びアプリケーションプログラムの実行による外部装置とのアクセスを第１又は第２無線通信用ドライバにより行わせる通信ステップと、

アプリケーションプログラムの終了時にデバイスドライバ、個人認証ライブラリ及びアプリケーションプログラムをアンインストールさせるアンインストールステップと、

を実行させることを特徴とする。

【００２８】

なお、本発明の情報処理方法及びプログラムの詳細は、情報処理デバイスと基本的に同じになる。

【００２９】

【発明の実施の形態】

図２は、本発明によるピアトークンと呼ばれる情報処理デバイスが適用されるシステム環境の説明図である。

【００３０】
図２において、本発明の処理デバイスはピアトークン１０として実現されている。ピアトークン１０は無線ＬＡＮとＰＨＳの二重化された通信機能を持ち、個人認証環境及びグループウェアシステム環境を不揮発メモリ上に内蔵したトークン型の外部ペリフラル装置である。

【００３１】
このピアトークン１０は、例えば出張先で使用することのできるパーソナルコンピュータで１２のＵＳＢ２ポートに差し込むことで、使用先となるパーソナルコンピュータ１２の環境を犯すことなく認証作業を行い、且つグループウェアシステム環境をパーソナルコンピュータ１２上に構築し、ピアツーピア型のグループウェアによる処理を可能とする。

【００３２】
このようなピアトークン１０の使用環境にあっては、ピアトークン１０の無線ＬＡＮ及びＰＨＳの通信機能を利用して、ＰＨＳ基地局２０または無線ＬＡＮに対応したホットスポット２２との間に通信回線を確立し、インターネット１６を経由して例えばプロキシサーバ１８を介したＬＡＮ１５に接続されているグループウェアに属するピア装置１４－１～１４－３や、インターネット１６に直接接続されるピア装置１４－４との間でデータを共有するグループウェアシステムを構築する。また、ピアトークン１０を使用先となるパーソナルコンピュータ１２に差し込んだ際の個人認証の処理に対応し、インターネット１６を介して認証サーバ２４が設けられている。

【００３３】
図３は、本発明によるキー型のピアトークン１０の外観を示している。ピアトークン１０は、樹脂成型されたパッケージによるデバイス本体２６をキー型に構成し、デバイス本体２６の一端にパーソナルコンピュータやＰＤＡなどの情報処理装置に接続するためのデバイスコネクタとして例えばＵＳＢ２コネクタ２８を設けている。

【００３４】
ここでＵＳＢ２インタフェースは、パーソナルコンピュータ及びＰＤＡ側のＵＳＢ２ポートに対するコネクタ接続でピアトークン１０に対し電源供給を行うと同時にデータ転送を行うことができる。

【００３５】
図４は、本発明によるピアトークン１０のハードウェア構成のブロック図である。図４において、ピアトークン１０にはパーソナルコンピュータやＰＤＡに差し込むためのＵＳＢ２コネクタ２８が設けられ、これに続いてＵＳＢ２インタフェース３０及びＭＰＵ３２が設けられている。

【００３６】
ＭＰＵ３２に対しては、不揮発メモリであるフラッシュメモリ３４が接続される。またＭＰＵ３２に対しては、外部装置との無線回線によるデータ転送を行うためＰＨＳ送受信部３６と無線ＬＡＮ送受信部３８が設けられている。

【００３７】
図５は、図４のフラッシュメモリ３４の格納内容となるメモリマップの説明図である。このメモリマップ４０に示すように、フラッシュメモリ３４には、デバイス処理プログラム４２、デバイスドライバ４４、アプリケーションプログラムとしてのグループウェア４６、個人認証ライブラリ４８、ＰＨＳドライバ５０、無線ＬＡＮドライバ５２及びＵＳＢドライバ５４が予め格納されている。

【００３８】
このようなプログラム領域に続く残りの領域はデータ領域５５となっており、この実施形態のアプリケーションであるグループウェアシステム環境の構築により送受信されたファイルデータが格納される。このデータ領域は、グループウェアシステム環境の場合には、右側に取り出して示すようにファイルリスト５６と実データ域５７で構成されている。

【００３９】
ここで、メモリマップ４０の先頭に格納されているデバイス処理プログラム４２は、ＭＰ

Ｕ３２による実行でピアトークン１０のＯＳとなるデバイス処理部として動作する。次のデバイスドライバ４４は、ピアトークン１０をパーソナルコンピュータやＰＤＡに差し込んだ際のピアトークン１０とのやり取りを行うためのプログラムであり、パーソナルコンピュータやＰＤＡ側にこのデバイスドライバ４４がない場合には、初期処理によりデバイスドライバ４４をインストールして、ピアトークン１０とのやり取りを行わせる。

【００４０】

グループウェア４６はアプリケーションプログラムであり、パーソナルコンピュータやＰＤＡ側にインストールされたデバイスドライバ４４の処理により差し込み先にダウンロードされてグループウェアシステム環境を作り、ピアツーピア型のデータ共有による送受信を行う。

【００４１】

個人認証ライブラリ４８は、グループウェア４６のインストールに先立つ個人認証処理のために差込み先にインストールされ、認証画面を開くことでユーザによるＩＤとパスワードの入力を受け、外部の認証サーバ２４とのやり取りで認証処理を行う。

【００４２】

ＰＨＳドライバ５０は図４のＰＨＳ送受信部３６を動作し、図２のようにＰＨＳ基地局２０との間に無線回線を確立して、ピアトークン１０の差込みで個人認証ライブラリ４８及びグループウェア４６がインストールされた使用先となるパーソナルコンピュータ１２のグループウェアシステム環境における例えば認証サーバ２４との間の認証のための通信、あるいはピア装置１４－１～１４－４との間のピアツーピアのデータ送受信を行う。

【００４３】

無線ＬＡＮドライバ５２は、図４の無線ＬＡＮ送受信部３８を制御し、図２のホットスポット２２との間で無線回線を確立し、同じくグループウェアシステム環境における個人認証処理や他のピア装置１４－１～１４－４との間のデータ共有のための送受信を行う。

【００４４】

このＰＨＳドライバ５０と無線ＬＡＮドライバ５２は、２つの無線回線を切り替えて使用するために設けられており、ピアトークン１０を差し込んだパーソナルコンピュータやＰＤＡの使用環境に応じ、いずれか一方の通信回線を自動的に選択して外部装置との間の送受信を行う。

【００４５】

図６は、本発明のピアトークン１０をパーソナルコンピュータ１２に差し込んでＵＳＢ２インタフェース６２による接続を確立した起動時の説明図である。パーソナルコンピュータ１２のＵＳＢに図３に示すピアトークン１０のＵＳＢ２コネクタ２８を差し込むと、パーソナルコンピュータ１２側からＵＳＢ２インタフェース６２の電源ラインを通じてピアトークン１０に電源供給が行われ、図４に示したピアトークン１０のハードウェアが起動し、図５のデバイス処理プログラム４２がＭＰＵ３２のメモリ領域に読み込まれて実行され、このデバイス処理プログラム４２の実行により、ＵＳＢドライバ５４、ＰＨＳドライバ５０及び無線ＬＡＮ５２が動作状態となる。

【００４６】

ピアトークン１０をパーソナルコンピュータ１２に差し込んだ際にパーソナルコンピュータ１２側にピアトークン１０のデバイスドライバ４４が存在しなかった場合には、図７のようなインストール要求画面４５がパーソナルコンピュータ１２側で表示され、デバイスドライバ４４のインストールを促す。

【００４７】

そこで、ユーザはインストール要求画面４５に続いてアイテム４５－１に示されている「一覧または特定の場所からインストールする」を選択して移行ボタン４５－２を操作すると、パーソナルコンピュータ１２のＵＳＢドライバ６０からピアトークン１０のＵＳＢドライバ５４にインストール要求のためのコマンドが転送され、図８のようにフラッシュメモリ３４からデバイスドライバ４４が読み出され、パーソナルコンピュータ１２のＯＳ５８の処理機能の１つとしてデバイスドライバ４４－１がインストールされる。

【００４８】
ピアトークン１０のデバイスドライバ４４－１がインストールされると、図9のようにデバイスドライバ４４－１によってピアトークン１０から個人認証ライブラリ４８－１がインストールされ、認証画面がパーソナルコンピュータ１２に表示される。

【００４９】
このためユーザは、認証画面の入力枠に対しＩＤとパスワードを入力して認証を要求すると、図２のようにＰＨＳ基地局２０またはホットスポット２２にある無線ＬＡＮのいずれかによる無線回線により認証サーバ２４に対し認証要求が行われ、正しいユーザであれば承認応答が得られる。

【００５０】
このような認証に成功すると、パーソナルコンピュータ１２側のデバイスドライバ４４－１は、図１０のようにピアトークン１０のグループウェア４６をパーソナルコンピュータ１２のＯＳ５８の配下のアプリケーションプログラムであるグループウェア４６－１としてインストールし、これによってグループウェアシステム環境がパーソナルコンピュータ１２側に構築される。

【００５１】
ここで、パーソナルコンピュータ１２はピアトークン１０を保有しているユーザが例えば出張などにより借用した装置であり、ピアトークン１０の差込みにより、借用したパーソナルコンピュータ１２上にユーザ個人のグループウェアシステム環境を個人の認証処理のみをもって簡単に構築することができる。

【００５２】
図１１は、パーソナルコンピュータ１２から本発明のピアトークン１０を外した際の説明図である。パーソナルコンピュータ１２にピアトークン１０を差し込んでグループウェアシステム環境による共有データの送受信や処理を行って作業を終了したならば、グループウェアシステム環境のアプリケーション終了を行った後にピアトークン１０をパーソナルコンピュータ１２から外し、ＵＳＢ２インタフェース６２による接続を切り離す。

【００５３】
このピアトークン１０の切り離しに先立ってグループウェアのアプリケーション終了操作が行われると、パーソナルコンピュータ１２からピアトークン１０に対し終了通知が行われ、ピアトークン１０側で必要な終了処理が行われると同時に、パーソナルコンピュータ１２側にあっては、図１１のようにパーソナルコンピュータ１２側にインストールされているデバイスドライバ４４－１、個人認証ライブラリ４８－１及びグループウェア４６－１のアンインストールが自動的に行われる。

【００５４】
またグループウェアシステム環境の構築で送受信されたデータについては、全てピアトークン１０のフラッシュメモリ３４に保存されている。このため、ピアトークン１０をパーソナルコンピュータ１２から外した場合、ピアトークン１０の差込みで構築した環境は全て削除され、ピアトークン１０によりパーソナルコンピュータ１２を利用しても、使用後にあってはパーソナルコンピュータ１２にピアトークン１０の使用による環境を一切残すことがなく、パーソナルコンピュータ１２の環境をピアトークン１０の使用で侵すことがない。

【００５５】
図１２は、本発明のピアトークン１０を出張先で借りた装置に接続した際の処理手順のフローチャートである。

【００５６】
図2において、ピアトークン１０をステップＳ１でパーソナルコンピュータ１２のＵＳＢ２ポートに接続すると、パーソナルコンピュータ１２にあっては、ステップＳ１０１でＵＳＢ２ポートに対するデバイスの存在を検知し、ピアトークン１０のデバイスドライバを持たない場合には、ステップＳ１０２でデバイスドライバのインストールを行う。

【００５７】

即ち、パーソナルコンピュータ１２は図７のようなインストール要求画面を表示し、このインストール要求画面に対するユーザの操作でデバイスドライバのインストール要求をピアトークン１０に対し行い、これを受けてピアトークン１０は、ステップＳ２でデバイスドライバをパーソナルコンピュータ１２に転送し、デバイスドライバがインストールされて実行される。

【００５８】

次にパーソナルコンピュータ１２側にあっては、インストールされたデバイスドライバの実行で、ステップＳ１０３において認証ライブラリのインストールを行う。即ち、ピアトークン１０に対し認証ライブラリのインストール要求を行い、これを受けてピアトークン１０は、ステップＳ３で個人認証ライブラリの転送を行い、パーソナルコンピュータ１２における認証ライブラリのインストールと実行が行われる。

【００５９】

認証ライブラリが実行されると、ステップＳ１０４で認証画面が表示され、この認証画面に対しユーザはＩＤとパスワードを入力することで、ピアトークン１０に対し認証要求を行う。ピアトークン１０は、ステップＳ４でＰＨＳまたは無線ＬＡＮ経由で認証要求のための送受信を外部の認証サーバとの間で行い、認証サーバから認証結果を受け、ステップＳ５で認証結果をパーソナルコンピュータ１２に通知する。

【００６０】

パーソナルコンピュータ１２にあっては、ステップＳ１０５で認証を取得した場合には、ステップＳ１０６以降の処理に進む。認証が取得できなかった場合には、ステップＳ１１０の処理に進む。認証を取得した場合には、まずステップＳ１０６でピアトークン１０からのグループウェアのインストールを行う。

【００６１】

即ち、ピアトークン１０に対しグループウェアのインストール要求を行い、これを受けてピアトークン１０がステップＳ６でグループウェアの転送を行い、パーソナルコンピュータ１２にグループウェアがインストールされて実行される。

【００６２】

このようにしてパーソナルコンピュータ１２でグループウェアシステム環境が構築されると、ステップＳ１０７で共有ファイルの同期処理を行う。共有ファイルの同期処理は、グループウェアシステム環境に属している他のピア装置との間で共有データが同じになるように差分データの転送によるマージ処理を行う。

【００６３】

この共有ファイルの同期処理に伴う他のピア装置との間のやり取りのため、ピアトークン１０にあっては、ステップＳ７のようにＰＨＳまたは無線ＬＡＮによる転送処理を行う。

【００６４】

続いてステップＳ１０８で、グループウェアシステム環境の構築の下にピアツーピアによるグループウェアの運用が行われる。このグループウェアの運用における他のピア装置との間のデータのやり取りについても、ピアトークン１０はステップＳ８のように、ＰＨＳまたは無線ＬＡＮによる転送処理を行う。

【００６５】

ステップＳ１０９でグループウェアの終了が判別されると、ステップＳ１１０で終了通知をピアトークン１０に対し行った後、ステップＳ１１１でピアトークン１０の差込みによりインストールしたデバイスドライバ、個人認証ライブラリ及びグループウェアのアンインストールを自動的に行う。

【００６６】

またピアトークン１０にあっては、パーソナルコンピュータ１２からの終了通知を受けて、ステップＳ９でポート切り離しに伴う電源断に対する終了処理を行う。最終的に、パーソナルコンピュータ１２からピアトークン１０をステップＳ１０で抜き外し、これによってパーソナルコンピュータ１２にあっては、ステップＳ１１２でＵＳＢ２ポートのデバイス存在を認識してＵＳＢの処理を終了させる。

【００６７】
図１３は、図１２のグループウェアシステム環境を構築した際のパーソナルコンピュータ１２のステップＳ１０７における共有ファイル同期処理の詳細を示したフローチャートである。

【００６８】
図１３において、共有ファイル同期処理は、ステップＳ１０１でピアトークン１０に対し保存ファイルの更新情報を要求する。これを受けてピアトークン１０にあっては、ステップＳ１でファイル名と更新情報をパーソナルコンピュータ１２に応答する。

【００６９】
続いてステップＳ１０２で、パーソナルコンピュータ１２はグループウェアに属する他のピア装置に対し、ピアトークン１０に保存している共有ファイルの更新情報を要求する。これを受けてピアトークン１０は、ステップＳ２でＰＨＳまたは無線ＬＡＮで他のピア装置に対し共有ファイルの更新情報をアクセスして結果を通知する。

【００７０】
続いてステップＳ１０３で、ピアトークン１０と他のピア装置とで更新日の異なるファイルについて他のピア装置に対し差分データの転送を要求し、これを受けてピアトークン１０は、ステップＳ３でＰＨＳまたは無線ＬＡＮで他のピア装置にアクセスし、差分データを取得する。

【００７１】
このため、ステップＳ１０４でピアトークン１０に対し差分データのマージによるファイル更新を指示する。これを受けてピアトークン１０は、ステップＳ４で他のピア装置から受信した差分データを対応する保存ファイルとマージすることでファイル更新を行う。

【００７２】
なおステップＳ４の差分データのマージはピアトークン１０側で行わず、パーソナルコンピュータ１２側で行って、結果をピアトークン１０のメモリに保存するようにしてもよい。

【００７３】
このようにピアトークン１０をパーソナルコンピュータ１２に差し込んでグループウェアシステム環境を構築すると、最初にピアトークン１０に保存している共有データの同期処理が行われるため、その後のグループウェアシステム環境でのファイル利用は常に最新のファイルを対象に行うことができる。

【００７４】
図１４は、グループウェアシステム環境がピアトークン１０の差込みで構築されたパーソナルコンピュータ１２におけるファイルアクセスの処理手順のフローチャートである。

【００７５】
まずステップＳ１０１でパーソナルコンピュータ１２側でのファイルオープンが行われると、このファイルオープン要求がピアトークン１０に伝えられ、ステップＳ１で該当ファイルをフラッシュメモリ３４から読み出して転送し、ステップＳ１０２で必要とするファイル処理を行う。

【００７６】
またステップＳ１０３で、オープンしたファイルのクローズが判別されると、ステップＳ１０４でファイルをピアトークン１０に転送し、フラッシュメモリ３４に格納する。

【００７７】
ここで、ステップＳ１０２のファイル処理においてオープンしたファイルについて新たなデータを追加するなどしてファイル容量が増加する場合があり、ファイルオープン時にはメモリ容量が十分であったものが、ファイルクローズに伴うメモリ格納時にはフラッシュメモリ３４のメモリ容量が不足する場合がある。

【００７８】
そこでピアトークン１０にあっては、ステップＳ１０４からファイルクローズに伴うファイル転送を受けると、ステップＳ２でメモリ容量が不足するか否かチェックする。もしメ

モリ容量が不足した場合にはステップＳ３に進み、図５のデータ領域５５に格納しているファイルリスト５６の末尾のファイルｎに対応したファイルｎデータを取得し、ステップＳ４で他のピア装置例えば図２におけるパーソナルコンピュータ１２に対し近隣となるピア装置１４－４に転送して保存する。

【００７９】

続いてステップＳ５でファイルｎの実データを消去し、ここに他のピア装置の保存を示すリンク情報を格納する置き換えを行う。このようにファイルｎのデータを消去してそのリンク情報に置き換えることで、リンク情報の必要容量はごく少ないことから実データ域５７に空き容量を確保できる。

【００８０】

そしてステップＳ６で、ファイルクローズに伴い転送された使用済みファイルをファイルリスト５６の先頭位置に格納する。もちろんファイルリストの末尾のファイルを１つ、他のピア装置に転送して実データを消去してもなおメモリ容量が不足する場合には、再度、末尾のファイルを削除してメモリ空き容量を確保する処理を、メモリ容量の不足が解消するまで繰り返すことになる。

【００８１】

このため、ピアトークン１０のメモリ容量に制約があっても、実データを他のピア装置に保存してそのリンク情報をピアトークン１０に保存することで、ピアトークン１０におけるメモリ容量不足の影響を受けることなく、グループウェアシステム環境において使用している共有データの実質的な保存と利用が実現できる。

【００８２】

図１５は、本発明のピアトークンを携帯電話に接続して、交通機関改札のゲートシステムや自動販売機の制御処理を行う他の実施形態の説明図である。

【００８３】

図１５において、携帯電話６１は、図２の実施形態におけるパーソナルコンピュータ１２の場合と同様、ＵＳＢ２ポートに相当するデバイスポートを持っており、ピアトークン１０の差込みで電源供給と同時にデータ転送を可能とする。

【００８４】

ピアトークン１０のフラッシュメモリには、例えば図１６のメモリマップ６８に示すように、図５のメモリマップ４０の内容に加えて新たに、ゲート処理プログラム７０と自動販売機処理プログラム７２が格納されており、ピアトークン１０の携帯電話６１に対する差込みでインストールされてアプリケーションプログラムとして動作させることができる。

【００８５】

図１７は、ゲートシステム６４を対象とした本発明のピアトークンと携帯電話の処理手順のフローチャートである。

【００８６】

図１７において、携帯電話６４にピアトークン１０を差し込んだ状態で交通機関の改札ゲートを通過しようとすると、ゲートの通信可能領域に入ったときにピアトークン１０はステップＳ１でゲートを認識し、ステップＳ２でゲート検知通知を携帯電話６１に送る。

【００８７】

これを受けて携帯電話６１側は、ステップＳ１０１でゲートイン要求をピアトークン１０に行い、ステップＳ３でＰＨＳまたは無線ＬＡＮによる無線送受信でゲートシステム６４に対しゲート要求を送り、応答結果を受信して携帯電話６４に返す。

【００８８】

このゲートイン要求に対し、ゲートシステム６４にあっては、改札ゲートを開くか、あるいはユーザの通過に対しロックを解除する。ゲートシステム６４からの応答情報には入場駅を示す入場情報が含まれていることから、ステップＳ１０２で入場情報を保持する。

【００８９】

このようにして改札ゲートに入った後は、ステップＳ４でピアトークン１０は再度、ゲート認識をチェックしており、利用者が到着駅のゲートから出ようとする際にゲート認識を

行って、ステップＳ５でゲート検知通知を携帯電話６１側に送る。これを受けて携帯電話６１は、ステップＳ１０３でゲートアウト要求をピアトークン１０のステップＳ６の無線送受信を介してゲートシステムに対し行い、このゲートアウト要求を受けてゲートシステム６４は、計算された料金データを応答する。

【００９０】

料金データを受けた携帯電話６１側にあっては、ステップＳ１０４で料金精算処理を行う。この料金精算処理は、予め保存しているプリペイド料金からの減額あるいは銀行口座から引き出している電子マネーの支払いなど、適宜の精算処理が行われる。

【００９１】

精算処理の結果はステップＳ７の無線送受信を通じてゲートシステム６４に通知され、精算確認応答を受けて、ステップＳ１０５で処理を終了し、一方、ゲートシステム６４にあっては精算確認に伴いゲート開あるいはゲートロック解除を行って、ユーザのゲート通過を可能とする。

【００９２】

図１８は、図１５の自動販売機６６を対象とした本発明のピアトークンと携帯電話における処理手順のフローチャートである。携帯電話６４に本発明のピアトークン１０を差し込んだ状態でユーザが自動販売機の前に立つと、ピアトークン１０はステップＳ１で自動販売機からの電波を受信して認識し、ステップＳ２で自動販売機の検知通知を携帯電話６１側に行う。

【００９３】

これに伴いユーザは、携帯電話６１を使用してステップＳ１０１で商品の購入要求を行う。例えば携帯電話６１の画面上に商品に選択画像が表示され、ユーザは購入したい商品を選択して実行要求することで、商品の購入要求がピアトークン１０のステップＳ３の無線送受信を通じて自動販売機に伝えられ、自動販売機より請求代金がピアトークン１０を介して携帯電話６１側に送られる。

【００９４】

そこで、ステップＳ１０２において購入代金の精算処理を行うと、プリペイド料金からの購入代金の残額あるいは銀行口座から引き落とした電子マネーの支払いがステップＳ４の無線送受信を通じて行われ、自動販売機から精算確認応答が得られると、ステップＳ１０３で終了処理を行う。

【００９５】

このような図１７における交通機関のゲート処理や図１８の自動販売機処理における代金精算結果はピアトークン１０のフラッシュメモリに保存され、ユーザが自分のパーソナルコンピュータの設置場所に戻ってピアトークンを差し込むと、ピアトークン１０に保存されている精算情報が自分のパーソナルコンピュータ側に転送されて自動的に編集され、ユーザの資産情報にマージするなどの処理を行わせることができる。

【００９６】

なお、グループウェアシステム環境における共有データの使い方として、自分のパーソナルコンピュータの実体データはサーバに保管しておき、サーバのファイル管理に使用しているネットワーク設定、各種アカウントなどのレジストリ情報をピアトークンに登録し、本発明のピアトークンを別のパーソナルコンピュータに挿入してレジストリ情報に基づくサーバからの共有ファイルの転送を行わせることで、本発明のピアトークンを別のパーソナルコンピュータに挿入すると同時に、自分が通常使用している作業環境を直ちに実現することができる。

【００９７】

また上記の実施形態は、ピアトークンに格納するアプリケーションとしてグループウェアプログラム、ゲート処理プログラム、自動販売機処理プログラムを例に取るものであったが、本発明はこれに限定されず、無線回線を利用して他の装置との間でデータのやり取りを行う適宜のアプリケーションをピアトークンに格納してパーソナルコンピュータやＰＤＡ、更には携帯電話に差し込むことで、差込み先の装置にアプリケーションプログラム環

境を構築して利用することができる。

【００９８】

また本発明は、その目的と利点を損なうことのない適宜の変形を含み、更に実施形態に示した数値による限定は受けない。

【００９９】

ここで本発明の特徴をまとめると次の付記のようになる。

（付記）

（付記１）

電源供給とデータ転送が可能な情報処理装置のデバイスポートに対し着脱自在なポートコネクタと、

外部装置に対し無線回線により情報を送受する第１無線通信部と、

外部装置に対し前記第１無線通信部とは異なる無線回線を使用して情報を送受する第２無線通信部と、

デバイスドライバ、ポートドライバ、個人認証ライブラリ、任意のアプリケーションプログラム、第１無線通信用ドライバ及び第２無線通信用ドライバを格納した不揮発メモリと、

前記ポートコネクタを情報処理装置のデバイスポートに接続した際に起動し、前記情報端末装置からの最初のデバイスアクセスに対し前記デバイスドライバを転送してインストールさせ、インストールされた前記デバイスドライバにより前記個人認証ライブラリをインストールさせて個人認証を行わせ、個人認証に成功した場合に前記アプリケーションプログラムをインストールして実行させ、前記認証ライブラリ及びアプリケーションプログラムの実行による外部装置とのアクセスを前記第１又は第２無線通信用ドライバにより行わせ、アプリケーションの終了時には前記デバイスドライバ、個人認証ライブラリ及びアプリケーションプログラムをアンインストールさせるデバイス処理部と、

を備えたことを特徴とする情報処理デバイス。（１）

【０１００】

（付記２）

付記１記載の情報処理デバイスに於いて、デバイス本体は持ち運び自在なキー型であることを特徴とする情報処理デバイス。

【０１０１】

（付記３）

付記１記載の情報処理デバイスに於いて、前記デバイスポートはＵＳＢ２ポートであり、前記ポートドライバはＵＳＢ２ドライバであることを特徴とする情報処理デバイス。

【０１０２】

（付記４）

付記１記載の情報処理デバイスに於いて、前記第１無線通信部はＰＨＳ無線回線を使用するＰＨＳ通信部であり、前記第２無線通信部は無線ＬＡＮを使用する無線ＬＡＮ通信部であることを特徴とする情報処理デバイス。

【０１０３】

（付記５）

付記１記載の情報処理デバイスに於いて、前記アプリケーションプログラムは複数の情報処理装置でデータを共有するピアツーピア型のグループウェア処理プログラムであることを特徴とする情報処理デバイス。（２）

【０１０４】

（付記６）

付記５記載の情報処理デバイスに於いて、前記アプリケーションプログラムがグループウェア処理プログラムの場合、前記個人認証ライブラリは前記第１又は第２無線通信部により外部の認証サーバに接続して認証処理を実行させることを特徴とする情報処理デバイス。

【０１０５】

（付記７）
付記１記載の情報処理デバイスに於いて、前記不揮発メモリに自己の情報処理装置で使用しているファイルをサーバに格納したことを示すディレクトリ情報を登録し、前記アプリケーションプログラムは、他の情報処理装置の差込み時に、前記レジストリ情報により前記サーバからファイルを取得して前記自己の情報処理装置の作業環境を構築することを特徴とする情報処理デバイス。（３）

【０１０６】
（付記８）
電源供給とデータ転送が可能な情報処理装置のデバイスポートに対し着脱自在なポートコネクタと、外部装置に対し無線回線により情報を送受する第１無線通信部と、外部装置に対し前記第１無線通信部とは異なる無線回線を使用して情報を送受する第２無線通信部と、デバイスドライバ、ポートドライバ、個人認証ライブラリ、任意のアプリケーションプログラム、第１無線通信用ドライバ及び第２無線通信用ドライバを格納した不揮発メモリとを備えたデバイスの情報処理方法に於いて、
前記ポートコネクタを情報処理装置のデバイスポートに接続した際に起動し、前記情報端末装置からの最初のデバイスアクセスに対し前記デバイスドライバを転送してインストールさせる起動ステップと、
インストールされた前記デバイスドライバにより前記個人認証ライブラリをインストールさせて個人認証を行わせる個人認証ステップと、
個人認証に成功した場合に前記アプリケーションプログラムをインストールして実行させる実行ステップと、
前記認証ライブラリ及びアプリケーションプログラムの実行による外部装置とのアクセスを前記第１又は第２無線通信用ドライバにより行わせる通信ステップと、
アプリケーションプログラムの終了時に前記デバイスドライバ、個人認証ライブラリ及びアプリケーションプログラムをアンインストールさせるアンインストールステップと、
を備えたことを特徴とする情報処理方法。（４）

【０１０７】
（付記９）
電源供給とデータ転送が可能な情報処理装置のデバイスポートに対し着脱自在なポートコネクタと、外部装置に対し無線回線により情報を送受する第１無線通信部と、外部装置に対し前記第１無線通信部とは異なる無線回線を使用して情報を送受する第２無線通信部と、デバイスドライバ、ポートドライバ、個人認証ライブラリ、任意のアプリケーションプログラム、第１無線通信用ドライバ及び第２無線通信用ドライバを格納した不揮発メモリとを備えたデバイスのコンピュータに、
前記ポートコネクタを情報処理装置のデバイスポートに接続した際に起動し、前記情報端末装置からの最初のデバイスアクセスに対し前記デバイスドライバを転送してインストールさせる起動ステップと、
インストールされた前記デバイスドライバにより前記個人認証ライブラリをインストールさせて個人認証を行わせる認証ステップと、
個人認証に成功した場合に前記アプリケーションプログラムをインストールして実行させる実行ステップと、
前記認証ライブラリ及びアプリケーションプログラムの実行による外部装置とのアクセスを前記第１又は第２無線通信用ドライバにより行わせる通信ステップと、
アプリケーションプログラムの終了時に前記デバイスドライバ、個人認証ライブラリ及びアプリケーションプログラムをアンインストールさせるアンインストールステップと、
を実行させることを特徴とするプログラム。（５）

【０１０８】
【発明の効果】
以上説明してきたように本発明によれば、キー型に形成された小型の情報処理デバイスを例えば出張先で使用することのできるパーソナルコンピュータのデバイスポートに差し込

むだけで、個人認証画面が自動的に立ち上がり、個人認証を済ませた後はグループウェアなどのアプリケーション画面が立ち上がり、外部との送受信を含む作業をすぐ始めることができる。

【０１０９】

また外部との通信に使用する無線通信機能がＰＨＳと無線ＬＡＮにより二重化されており、使用場所の無線環境に対応して有効な側に自動切替して外部に確実にアクセスすることができる。

【０１１０】

更に、情報処理デバイスの差込みによるアプリケーションの実行で使用されたデータは全てデバイス側の不揮発メモリに保存され、また情報処理デバイスを抜いて処理を終えると、パーソナルコンピュータなどの差込み側の装置にはインストールしたプログラムやドライバは全てアンインストールされて残ることがなく、差込み先の装置の環境を全く侵すことなく、本発明の情報処理デバイスの差込みによるアプリケーション環境の利用が実現できる。

【図面の簡単な説明】

【図１】本発明の原理説明図

【図２】本発明が適用されたシステム環境の説明図

【図３】本発明によるキー型ピアトークンの外観の説明図

【図４】本発明によるピアトークンのハードウェア構成のブロック図

【図５】図４の不揮発メモリの格納内容となるメモリマップの説明図

【図６】本発明のピアトークンを使用先となるパーソナルコンピュータに接続した起動時の説明図

【図７】ピアトークンの接続による使用先となるパーソナルコンピュータのインストール要求画面の説明図

【図８】図６に続いて使用先となるパーソナルコンピュータにデバイスドライバがインストールされた説明図

【図９】図８に続いて使用先となるパーソナルコンピュータに個人認証ライブラリがインストールされた説明図

【図１０】図９に続いて使用先となるパーソナルコンピュータにグループウェアがインストールされた説明図

【図１１】使用先となるパーソナルコンピュータのデバイスポートから本発明のピアトークンを外した際の説明図

【図１２】本発明のピアトークンを使用先となるパーソナルコンピュータに接続した際の処理手順のフローチャート

【図１３】共有ファイル同期処理における本発明のピアトークンと使用先となるパーソナルコンピュータの処理手順のフローチャート

【図１４】ファイルアクセスにおける本発明のピアトークンと使用先となるパーソナルコンピュータの処理手順のフローチャート

【図１５】本発明のピアトークンを携帯電話に接続して交通機関改札のゲートシステムや自動販売機の制御処理を行う実施形態の説明図

【図１６】図６のピアトークンにおける不揮発メモリのメモリマップ説明図

【図１７】ゲートシステムを対象とした本発明のピアトークンと携帯電話の処理手順のフローチャート

【図１８】自動販売機を対象とした本発明のピアトークンと携帯電話の処理手順のフローチャート

【符号の説明】

１０：ピアトークン（情報処理デバイス）

１２：パーソナルコンピュータ

１４－１～１４－４：ピア装置

１５：ＬＡＮ

１６：インターネット

１８：プロキシサーバ

２０：ＰＨＳ基地局

２２：ホットスポット（無線ＬＡＮ）

２４：認証サーバ

２６：デバイス本体

２８：ＵＳＢ２コネクタ

３０，６２：ＵＳＢ２インタフェース

３２：ＭＰＵ（プロセッサ）

３４：フラッシュメモリ（不揮発メモリ）

３６：ＰＨＳ送受信部

３８：無線ＬＡＮ送受信部

４０，６８：メモリマップ

４２：デバイス処理プログラム（トークンＯＳ）

４４：デバイスドライバ

４５：インストール要求画面

４６：グループウェア

４８：個人認証ライブラリ

５０：ＰＨＳドライバ

５２：無線ＬＡＮドライバ

５４，６０：ＵＳＢドライバ

５５：データ領域

５６：ファイルリスト

５７：実データ域

５８：使用先となるパーソナルコンピュータＯＳ

６１：携帯電話

６４：ゲートシステム

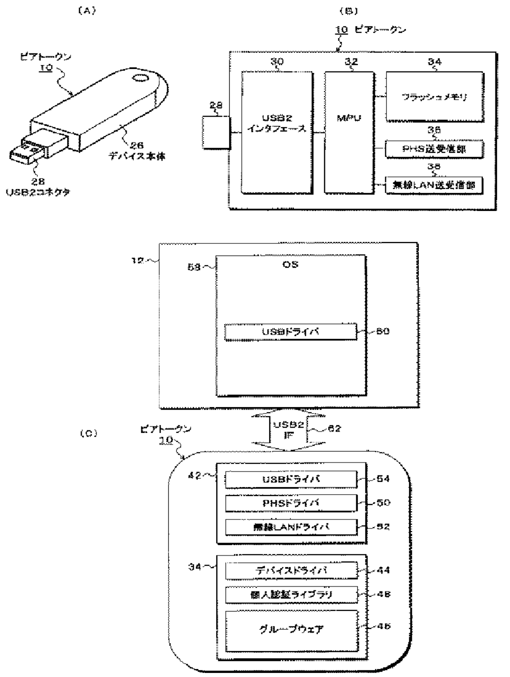
６６：自動販売機

７０：ゲート処理プログラム

７２：自動販売機処理プログラム

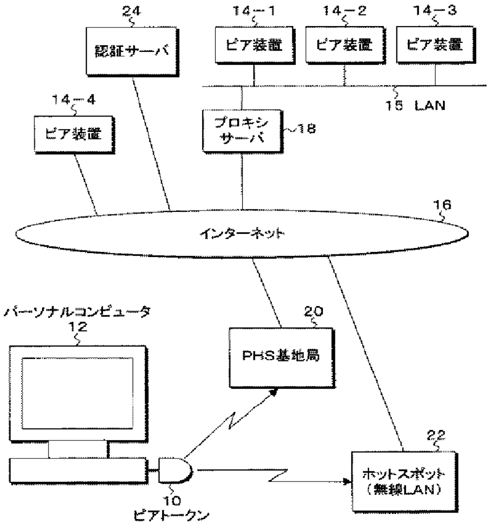
【図1】

本発明の原理説明図



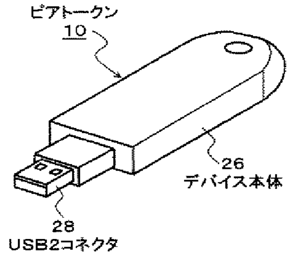
【図2】

本発明が適用されたシステム環境の説明図



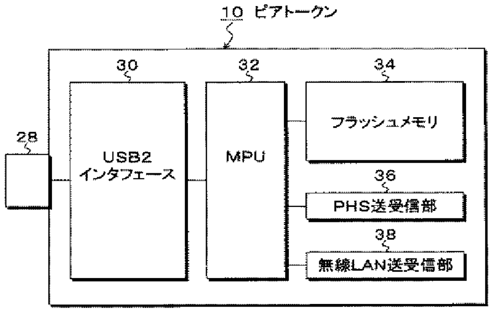
【図3】

本発明によるキー型ピアトークンの外観の説明図



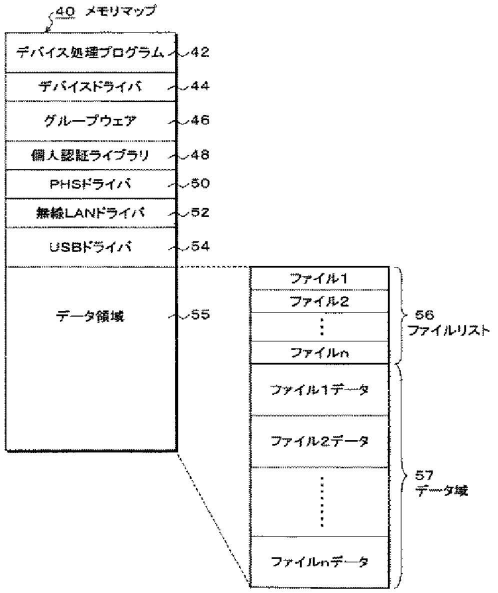
【図4】

本発明によるピアトークンのハードウェア構成のブロック図



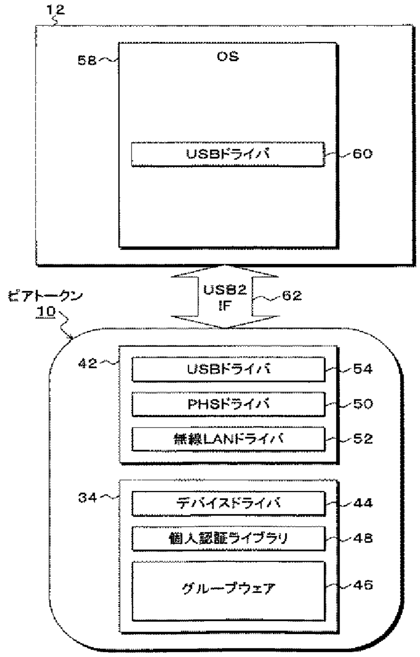
【図5】

図4の不揮発メモリの格納内容となるメモリマップの説明図



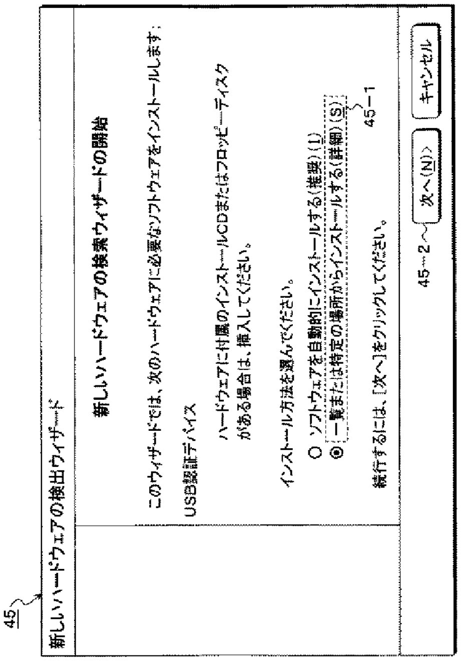
【図6】

本発明のピアトークンを使用先のパーソナルコンピュータに接続した起動時の説明図



【図7】

ピアトークンの接続による使用先のパーソナルコンピュータのインストール要求画面の説明図



新しいハードウェアの検索ウィザードの開始

このウィザードでは、次のハードウェアに必要なソフトウェアをインストールします：

USB認証デバイス

ハードウェアに付属のインストールCDまたはフロッピーディスクがある場合は、挿入してください。

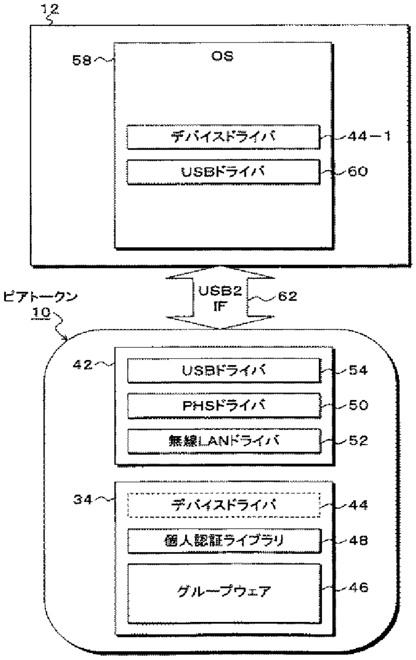
インストール方法を選んでください。

○ ソフトウェアを自動的にインストールする（推奨）（I）
◉ 一覧または特定の場所からインストールする（詳細）（S）

続行するには、［次へ］をクリックしてください。

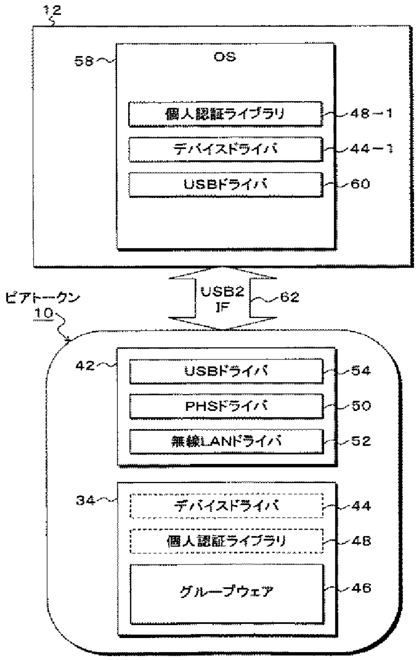
【図8】

図6に続いて使用先のパーソナルコンピュータにデバイスドライバがインストールされた説明図



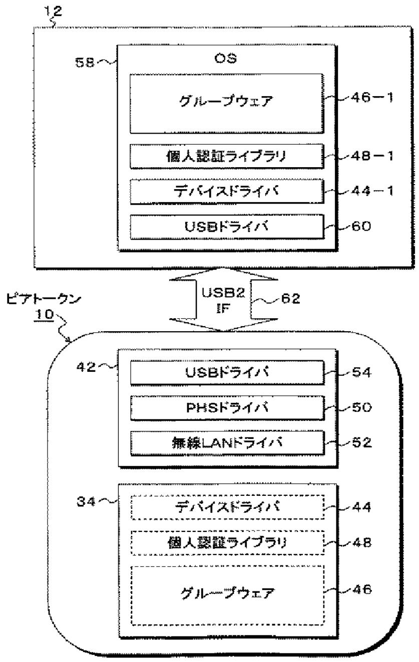
【図9】

図8に続いて使用先のパーソナルコンピュータに個人認証ライブラリがインストールされた説明図



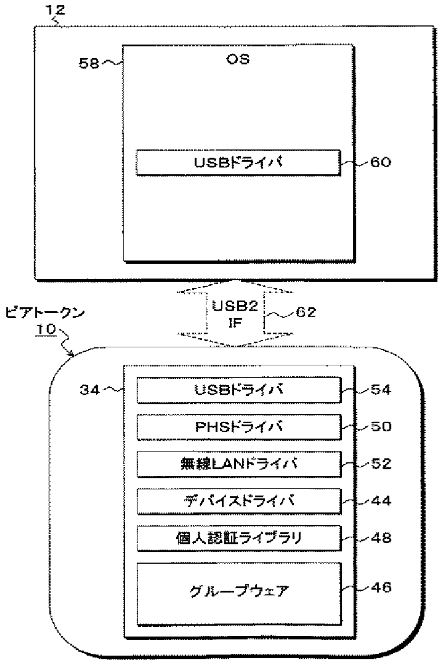
【図10】

図9に続いて使用先のパーソナルコンピュータにグループウェアがインストールされた説明図



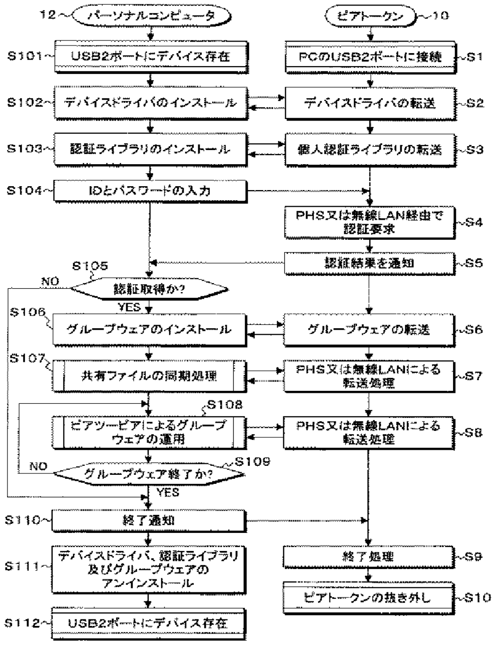
【図11】

使用先のパーソナルコンピュータのデバイスポートから本発明のピアトークンを外した際の説明図



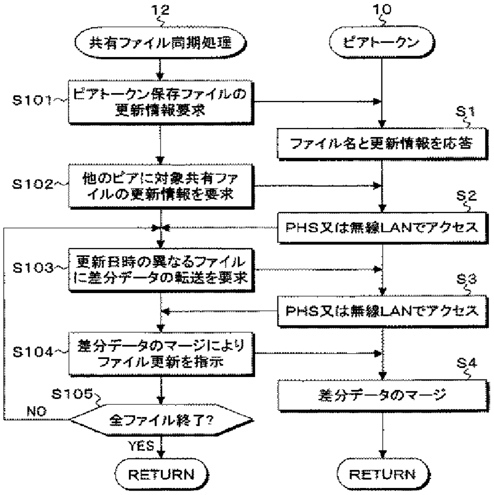
【図12】

本発明のピアトークンを使用先のパーソナルコンピュータに接続した際の処理手順のフローチャート



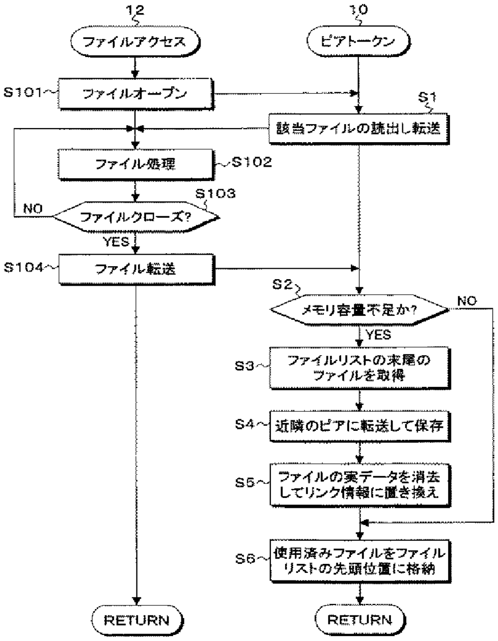
【図13】

共有ファイル同期処理における本発明のピアトークンと使用先のパーソナルコンピュータの処理手順のフローチャート


12
共有ファイル同期処理
10
ピアトークン
S101
ピアトークン保存ファイルの更新情報要求
S1
ファイル名と更新情報を応答
S102
他のピアに対象共有ファイルの更新情報を要求
S2
PHS又は無線LANでアクセス
S103
更新日時の異なるファイルに差分データの転送を要求
S3
PHS又は無線LANでアクセス
S104
差分データのマージによりファイル更新を指示
S4
差分データのマージ
S105
NO
全ファイル終了?
YES
RETURN
RETURN

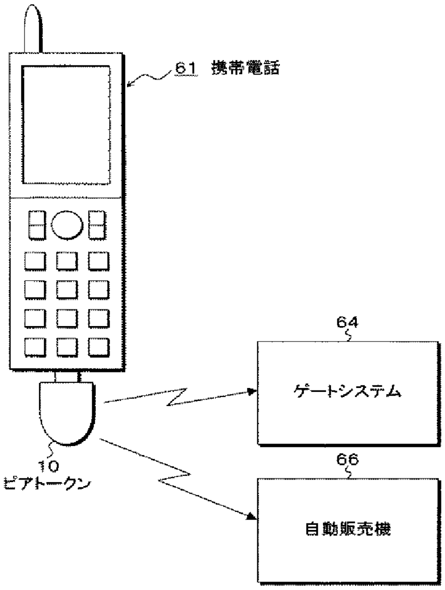
【図14】

ファイルアクセスにおける本発明のピアトークンと使用先のパーソナルコンピュータの処理手順のフローチャート



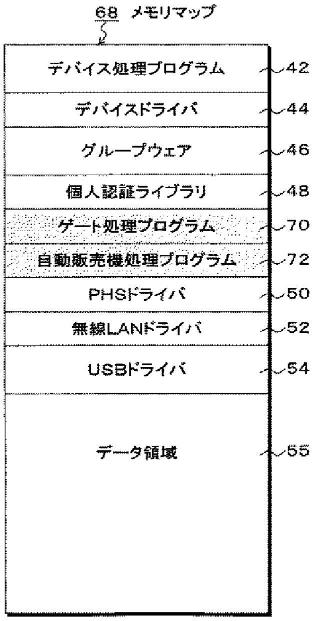
【図15】

本発明のピアトークンを携帯電話に接続して交通機関改札のゲートシステムや自動販売機の制御処理を行う実施形態の説明図



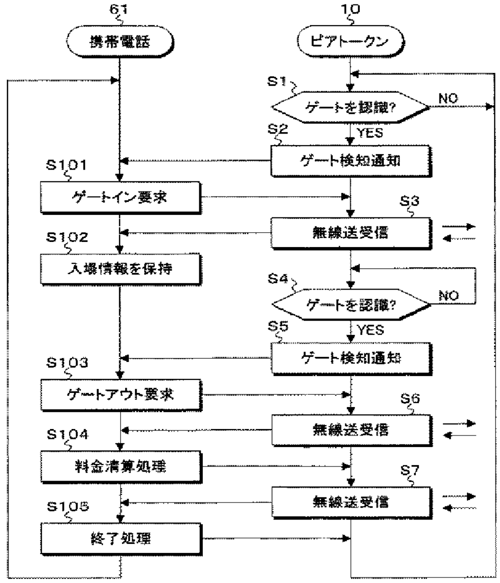
【図16】

図6のピアトークンにおける不揮発メモリのメモリマップ説明図



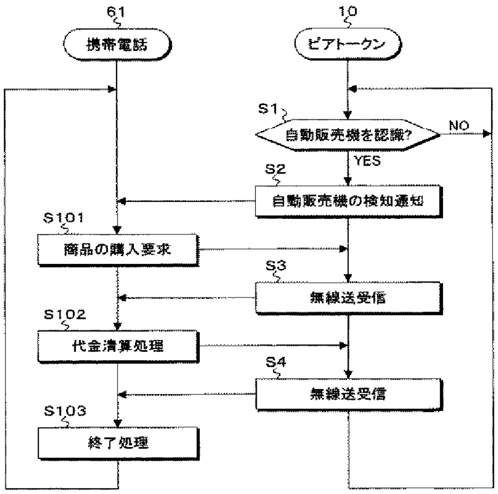
【図17】

ゲートシステムを対象とした本発明のピアトークンと携帯電話の処理手順のフローチャート



【図18】

自動販売機を対象とした本発明のピアトークンと携帯電話の処理手順のフローチャート



(51)Int.Cl.^{7}	ＦＩ	テーマコード（参考）
	Ｇ０６Ｆ　9/06　６６０Ｅ	

Ｆターム(参考) 5B014 FA14
5B076 AB20 BA05 BA10 BB12 BB18 FB01
5B085 AA04 AE02 AE12 AE23 BE01 BE04 BG01 BG02 BG07

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) **International Patent Classification** 6 :
G06F 17/60, G07F 7/02

A1

(11) **International Publication Number:** **WO 99/52051**

(43) **International Publication Date:** 14 October 1999 (14.10.99)

(21) **International Application Number:** PCT/GB99/00575

(22) **International Filing Date:** 25 February 1999 (25.02.99)

(30) **Priority Data:**
09/054,844 3 April 1998 (03.04.98) US

(71) **Applicant:** INTERNATIONAL BUSINESS MACHINES CORPORATION [US/US]; New Orchard Road, Armonk, NY 10504 (US).

(71) **Applicant** *(for MC only)*: IBM UNITED KINGDOM LIMITED [GB/GB]; P.O. Box 41, North Harbour, Portsmouth, Hampshire PO6 3AU (GB).

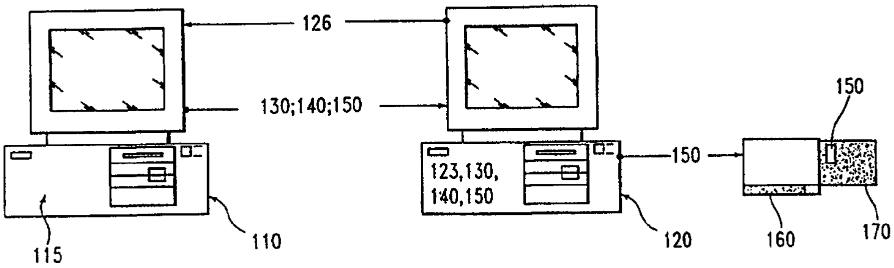
(72) **Inventors:** PALMER, Charles, Campbell; 293 Waccabuc Road, Goldens Bridge, New York, NY 10526 (US). PALMER, Elaine, Rivette; 293 Waccabuc Road, Goldens Bridge, New York, NY 10526 (US). SMITH, Sean, William; 19 Bridge Street, Cornwall, New York, NY 12518 (US).

(74) **Agent:** WILLIAMS, Julian, David; IBM United Kingdom Limited, Intellectual Property Dept., Hursley Park, Winchester, Hampshire SO21 2JN (GB).

(81) **Designated States:** CN, HU, JP, KR, PL, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) **Title:** AUTHENTICATED ELECTRONIC COUPON ISSUING AND REDEMPTION



(57) Abstract

An online coupon issuing and redemption system and method receives requests for coupons from consumers, presents advertisements and issues coupons to consumers electronically. The system presents advertisements before issuing the coupons, such that an issuer may be assured its targeted consumer is receiving its advertisements. The coupons are issued on a smart card, thereby eliminating a need for paper coupons. The coupons are digitally signed in order to prevent fraud. In order to prevent further fraudulent tampering of coupons, the redemption station includes a tamper–protected coprocessor for performing operations on the coupons. The system further includes capability for the redemption station to link to an issuing station for electronic reimbursements.

FOR THE PURPOSES OF INFORMATION ONLY

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

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

AUTHENTICATED ELECTRONIC COUPON ISSUING AND REDEMPTION

The present invention relates to an electronic advertisement and coupon issuance and redemption.

Retailers and manufacturers often sponsor incentive programs for persuading consumers to buy their products. These incentives include discount coupons distributed to consumers whereby a consumer may redeem the coupon when purchasing an associated item. Such coupons are usually distributed in paper forms.

The problems associated with paper coupons today are that the retailer and manufacturers who advertise cannot assure that consumers who use paper coupons have actually read the product advertisements which accompany the coupons. The advertisers do not have a way of knowing who is viewing their advertisements and cannot dynamically adjust the advertisement to fit the viewer's tastes and interests.

In addition, many cases of fraud related to paper coupons are occurring today. For example, paper coupons are easily counterfeited. Some consumers commit fraud by redeeming coupons for merchandise they have not purchased. Some retailers also commit fraud by redeeming coupons for merchandise which consumers have not purchased.

Manufacturers must rely on the cashiers and computer systems at retail establishments to assure that consumers who redeem coupons have actually bought the targeted product and that the coupons redeemed were not expired at the time of redemption. Retailers often rely on their cashiers to enforce coupon redemption rules. Other retailers rely on computerized systems to compare coupon bar codes to the consumer's purchases.

U.S. patent number 4880964 by Donahue describes paper coupons with bar codes printed on them, and thus does not solve the deficiencies of paper coupons described above. U.S. patent number 5710866 by Christensen et al. describes electronically generated coupons but requires a database of customers and spent coupons which is costly to maintain. It also requires online connection to the database at redemption time to determine if the coupon is valid.

In accordance with the present invention, there is now provided a coupon issuing system for electronically presenting advertisements and generating coupons, said system comprising: at least one issuing station for generating and transmitting electronic advertisements and electronic coupons according to predetermined criteria; at least one customer station to transmit from a user to the issuing station a request for an electronic coupon, for receiving electronic advertisements and electronic coupons from the issuing station, and for presenting the advertisement to the user for interaction with the user; at least one smart card for holding information including said electronic coupons; at least one smart card reader/writer for communicating information held in said at least one smart card to said at least one customer station; and at least one software program to monitor a status of the interaction of the user with the advertisement; whereby when said at least one software program detects a predefined status, said at least one software program transfers said electronic coupons to said smart card via said smart card reader/writer.

Viewing the present invention from another aspect, there is now provided a system for redeeming electronic coupons comprising: at least one redemption station; and at least one smart card reader/writer linked to said redemption station; whereby said redemption station selects and updates via said at least one smart card reader/writer, coupons stored in a smart card, deleting expired coupons and also those matching purchased items.

Viewing the present invention from yet another aspect, there is now provided a method for advertising and issuing at least one coupon electronically, said method comprising: receiving a request for said electronic coupon from a consumer; generating at least one electronic advertisement and said electronic coupon; transmitting said electronic advertisement and said electronic coupon to a consumer's station for presentation to said consumer; monitoring said consumer's interaction with said advertisement; and transferring said electronic coupon to a smart card, if said consumer's interaction with said advertisement meets a predefined status.

In a preferred embodiment of the present invention there is provided an online coupon issuing and redemption system. The issuing system includes an issuing station. The issuing station is generally comprised of a computer located usually at a manufacturer's site. The issuing station typically generates advertisements and coupons electronically. The issuing system also includes a consumer station, usually a computer and a smart card reader/writer generally located at the consumer site. The smart card reader/writer may be linked to the consumer computer either directly or via a LAN or other network connections.

The issuing station and consumer station are linked via a communications network. When a consumer makes requests via the consumer station for coupons, the issuing station transmits the advertisement and coupons it generated to the consumer station. The issuing station also has a capability of digitally signing the coupons. Digital signatures insure the authenticity of the coupons as well as that of the issuer and the issuing station. Also included in the transmission is a program having a capability to run on the consumer station. The program is responsible for making sure that the consumer absorbs the entire advertisement and transferring the coupons to a smart card via the smart card reader/writer linked to the consumer station.

This assures the advertisers that a consumer actually perceives the advertisement for a product before receiving discount coupons.

The redemption system generally comprises a redemption station, typically a computer, and a smart card reader/writer linked to the redemption computer. The redemption system is typically located at a purchasing site. When a consumer is ready to make a purchase, the consumer inserts the smart card having electronic coupons stored in it into the smart card reader/writer linked to the redemption station. The redemption system reads the coupons via the smart card reader/writer and matches the purchased items with coupons. The matched coupons are extracted from the smart card, so that they may not be used again. At the same time, the redemption system deletes any expired coupons stored in the smart card.

The redemption system also may include a tamper-protected secure coprocessor. In order to protect a manufacturer from fraudulent merchants and customers, operations which assess the validity of coupons, operations which update, collect, store, or delete coupons may take place inside a tamper-protected hardware boundary. The hardware boundary is part of typical tamper-protected secure coprocessors and smart cards.

This provides a tamper-protected access to the coupons stored in the smart cards.

Embodiments of the present invention may include a database of coupons stored in the issuing station. The database may include a list of coupons issued or already spent. When a consumer is ready to redeem the coupons, the redemption station links to the database and validates the coupons stored in the consumer's smart card by comparing the smart card coupons with a list of coupons in the database. Only the valid coupons matching the list in the database may be actually redeemed.

In embodiments of the present invention there may be provided a communications link between a redemption station and an issuing station. Such a link is established when a merchant wants reimbursements from the manufacturer for the coupons the merchant redeemed to the consumers.

Typically the redemption computer sends electronic coupons which have been digitally signed to the issuing computer. The issuing computer validates the electronic signatures on the coupon. If the signatures are valid, the manufacturer reimburses the merchants for the valid coupons. This provides a mechanism for the manufacturer to electronically reimburse the merchants.

Preferred embodiments of the present invention will now be described by way of example only, with reference to the accompanying drawings, in which:

Figure 1 is an exemplary diagram illustrating a physical architecture of an issuing system embodying the present invention;

Figure 2 is a flow diagram illustrating one possible logic flow of issuing software running on the issuing computer embodying the present invention;

Figure 3 is a flow diagram illustrating one possible logic flow of advertisement viewing software running on the viewing computer embodying the present invention;

Figure 4 is a flow diagram illustrating one possible logic flow for interaction between advertisement viewing software and issuing software;

Figure 5 is an illustrative example showing a physical layout of a redemption system architecture embodying the present invention;

Figures 6 and 7 are a flow diagram illustrating one possible logic flow in the redemption system during a typical point of sale;

Figure 8 is a flow diagram illustrating a possible logic flow in a typical daily coupon close-out;

Figure 9 is an illustrative example showing a physical layout of a software-based redemption system embodying the present invention.

Figure 1 is an exemplary diagram illustrating a physical architecture of an issuing system embodying the present invention. An authenticated electronic coupon issuing system shown in Figure 1 includes an issuing station, typically a computer 110 running issuing software 115; a viewing station, typically an advertisement viewing computer 120 running advertisement viewing software 123 which sends requests for coupons 125 to an issuing computer 110; an advertisement viewing computer 120 running advertisement applet software 130; an electronic advertisement 140; an electronic coupon which is digitally signed 150; a dispensing smart card reader/writer 160; a customer's smart card 170 holding an electronic coupon 150. A typical smart card may be a chip card having an integrated circuit that is resistant to physical tampering. An issuing station typically comprises a computer at a manufacturer or clearing house site. Likewise, a viewing station typically comprises of a computer at a customer site. A customer is typically a consumer who receives coupons electronically and makes purchases using the coupons.

A dispensing smart card reader/writer 160 is attached to an advertisement viewing computer 120 and is accessible by advertisement applet software 130.

Issuing software 115, advertisement viewing software 123, and advertisement applet software 130 are typically purchased from software vendors. An electronic advertisement 140 is supplied by an advertisement content vendor. A customer's smart card 170 may be purchased from a smart card vendor. Likewise, a customer's smart card reader/writer 160 may be supplied by a smart card reader/writer vendor. An issuing computer 110 and an advertisement viewing computer 120 may be obtained from computer hardware vendors. An electronic coupon 150 is generated by issuing software 115. A request for coupons 125 is generated by advertisement viewing software 123.

Figure 2 is a flow diagram illustrating one possible logic flow of issuing software running on the issuing computer of the present invention. Initially in step 210, the issuing software awaits a request from an advertisement viewing computer. A request includes information about the customer, such as his interests (e.g., propensity for playing tennis), and demographics (e.g., a senior citizen). In step 220, the issuing software retrieves a customer's interest profile and demographics from a request. In step 230, the issuing software selects an electronic advertisement which matches a customer's interest profile and demographics. For example, if a customer is a senior citizen, the issuing software selects an electronic advertisement targeted at senior citizens, not one targeted at teenagers. In step 240, the issuing software generates an electronic coupon which is digitally signed.

Digital signatures are generally created by piping a sender's private key and the contents of the message into an algorithm. The output of the algorithm is the digital signature. The recipient can verify the digital signature by using the sender's public key and the message. The digital signature is secure because it would be virtually impossible for another computer to produce the identical digital signature. Each user has the responsibility of protecting the private key.

In step 250, the issuing software transmits an electronic advertisement, advertisement applet software, and an electronic coupon to an advertisement viewing computer. The issuing software then waits for another request from the advertisement viewing software.

Figure 3 is a flow diagram illustrating one possible logic flow of advertisement viewing software running on the viewing computer of the present invention. In step 310, the advertisement viewing software awaits a request for a coupon from a customer. In step 315, the viewing software obtains information about a customer, such as his interests and demographics. The viewing software may obtain the information directly from a customer through a dialogue, or from a customer's smart card, or from a file on the viewing computer. In step 320, the viewing software includes a customer's interest profile and demographics with a request for a coupon. In step 325, the viewing software transmits a request for a coupon to an issuing computer. In step 330, the viewing software awaits a response from an issuing computer. If there is no response, the viewing software times out, in step 335, displays an error message and, in step 310, awaits for another request from a customer. If there is a response from an issuing computer, the viewing software receives advertisement applet software, an electronic advertisement, and an electronic coupon as shown in step 340. In step 350, the viewing software then runs advertisement applet software. The software determines, in step 360, if the customer viewed an entire advertisement. In step 370, if the applet software times out or if a customer exited the software prematurely, the viewing software terminates the session and returns to wait for another request from a customer in step 310. In step 380, if the applet determines that a customer did view the entire advertisement, the applet software transmits an electronic coupon which is digitally signed to a customer's smart card via a dispensing smart card reader/writer.

An example of viewing software may include a World Wide Web (Web) page having a uniform resource locator (URL) address which a consumer may access via a Web browser. The URL address would be located in the web server linked to an issuing station. The Web page may have a number of parameter fields as input fields which the consumer is required to fill. The Web page with the parameters may then be transmitted to the web server at the issuing station. The web server together with issuing software may then use the parameters to generate electronic advertisements and coupons, transmitting them with an applet software to the viewing software. The viewing software typically launches the applet software. The launched applet software displays the advertisements on the consumer station, controlling the station's interaction with the consumer. The applet software may also be responsible for transferring the coupons to the consumer's smart card. Furthermore, the applet software may provide interactivity, for example, requiring that the consumer answer questions about the product or advertisement, to assure that the consumer is truly absorbing the advertising information.

Figure 4 is a flow diagram illustrating one possible logic flow for interaction between advertisement viewing software and issuing software. In step 420, an advertisement viewing computer requests an electronic coupon from an issuing computer. In step 430, an issuing computer transmits advertisement applet software, an electronic advertisement, and an electronic coupon which is digitally signed to an advertisement viewing computer. In step 440, an advertisement viewing computer runs applet software. The applet software displays an electronic advertisement. In step 450, the applet software determines how to proceed based on whether or not a customer viewed an entire advertisement. In step 460, if a customer does not view an entire electronic advertisement, the advertisement applet software terminates the session and awaits another request, step 410. If, however, a customer views an entire electronic advertisement, in step 470, the applet software rewards the customer by transmitting an electronic coupon which is digitally signed to a customer's smart card. The smart card is typically inserted into a dispensing smart card reader/writer. Furthermore, the advertisement applet software may be interactive, requiring that a customer answer questions about a product or advertisement, to assure that a customer is truly absorbing the advertising information. Secure protocols, tamper-protected hardware, or record keeping databases typical in electronic money systems may be employed to prevent consumers and retailers from double spending or duplicating the electronic coupons. A suitable example for such secure protocols are described in detail in M. Bellare et al., "iKP - A Family of Secure Electronic Payment Protocols", July 12, 1995, available from IBM.

Electronic coupons are not printed, therefore they cannot be printed over and over again, or photocopied. The number of electronic coupons a smart card may hold may be limited.

Figure 5 is an illustrative example showing a physical layout of a redemption system architecture embodying the present invention. An authenticated coupon redemption system as shown in Figure 5 comprises a redemption computer 510, a tamper-protected secure coprocessor 520, a redemption smart card reader/writer 530, a customer's smart card storing a digitally signed electronic coupon 150, and an issuing station. An issuing station is typically comprised of a computer 110 and is generally resident at a manufacturer or at a clearing house that performs the duties for a manufacturer or a group of manufacturers. A redemption smart card reader/writer 530 is typically attached to a redemption computer 510. A tamper-protected secure coprocessor 520 is connected to a redemption computer 510 either directly or via a communications network. A redemption computer 510 may also be connected to an issuing computer 110, typically via phone line 570.

Figures 6 and 7 are a flow diagram illustrating a possible logic flow in the redemption system during a typical point of sale. In step 610, a consumer inserts the smart card 170 Figure 1 into a redemption smart card reader/writer 530 Figure 5. The smart card includes electronic coupons which have been digitally signed 150 Figure 1. In step 620, the smart card sends a list of all coupons stored in it to a redemption computer 510 Figure 5. In step 630, a redemption computer forwards the list of coupons and optionally a list of items purchased to a tamper-protected secure coprocessor 520 Figure 5. In step 640, the tamper-protected secure coprocessor 520 Figure 5 examines the list of all coupons, and assembles a list of those which have expired. In step 650, the tamper-protected secure coprocessor 520 Figure 5 requests a redemption computer to send a command to a smart card to delete expired coupons. Next, in step 660, the tamper-protected secure coprocessor searches for non-expired coupons that match actual items purchased. If there are no matching items, in step 670, the tamper-protected secure coprocessor tells the redemption computer that no items matched the coupon list. If there are matching items, in step 680, the tamper-protected secure coprocessor assembles a list of matching items and valid coupons. In step 690, the coprocessor requests the redemption computer to send a command to the smart card to extract valid matching coupons. In step 695, the smart card sends the valid matching coupons to the tamper-protected secure coprocessor.

In order to protect a manufacturer from fraudulent merchants and customers, operations which assess the validity of coupons, operations which update, collect, store, or delete coupons take place inside a tamper-protected hardware boundary 655. The hardware boundary is part of typical tamper-protected secure coprocessors and smart cards. A typical tamper-protected secure coprocessor may be a tamper-protected computing device having a microprocessor and memory in a tamper-protected enclosure, such as the IBM 4758.

Figure 8 is a flow diagram illustrating a possible logic flow during a typical daily coupon close-out. In step 710, a redemption computer 510 Figure 5 connects to the issuing computer 110 Figure 5 or clearing house computer. Such connection would generally occur at the end of the day, or at some appropriate period of time. In step 720, the redemption computer 510 Figure 5 sends electronic coupons which have been digitally signed 150 Figure 5 to the issuing computer 110 Figure 5. In step 730, the issuing computer validates the electronic signatures on the coupons. In step 740, the clearing house reimburses the merchant for the valid coupons.

Figure 9 is an illustrative example showing a physical layout of a software-based redemption system embodying the present invention. The embodiment shown in Figure 9 replaces the tamper-protected secure coprocessor 520 Figure 5 in the redemption computer 510 Figure 5 with a database of coupons 810 in the issuing computer 110 Figure 5. The database includes either a list of already spent coupons (so as to reject them if they are presented a second time) or a list of unspent coupons, from which it deletes coupons as they are presented for redemption. When a merchant connects to the issuing computer 110 to redeem the coupons, the issuing computer 110 searches the database 810 to determine if the coupons are valid. Only the valid coupons found in the database 810 may then be redeemed.

While the invention has been particularly shown and described with respect to a preferred embodiment thereof, it will be understood by those skilled in the art that the foregoing and other changes in form and details may be made therein without departing from the scope of the invention.

Claims

1. A coupon issuing system for electronically presenting advertisements and generating coupons, said system comprising:

at least one issuing station for generating and transmitting electronic advertisements and electronic coupons according to predetermined criteria;

at least one customer station to transmit from a user to the issuing station a request for an electronic coupon, for receiving electronic advertisements and electronic coupons from the issuing station, and for presenting the advertisement to the user for interaction with the user;

at least one smart card for holding information including said electronic coupons;

at least one smart card reader/writer for communicating information held in said at least one smart card to said at least one customer station; and

at least one software program to monitor a status of the interaction of the user with the advertisement;

whereby when said at least one software program detects a predefined status, said at least one software program transfers said electronic coupons to said smart card via said smart card reader/writer.

2. A system as claimed in claim 1, wherein said system further includes a user interface program for displaying information including request forms and the advertisements, whereby the advertisements are presented visually to the user via the customer station.

3. A system as claimed in claim 2, wherein said user interface program comprises a Web browser running on the customer station.

4. A system as claimed in claim 3, wherein said at least one software program includes a platform independent program downloadable dynamically from said issuing station, said at least one software program further controlling displays in conjunction with said Web browser.

5. A system as claimed in claim 1, wherein said issuing station digitally signs said electronic coupons before downloading said electronic coupons to said customer station.

6. A system as claimed in claim 1, wherein said advertisements are updated over predefined intervals.

7. A system for redeeming electronic coupons comprising:

at least one redemption station; and

at least one smart card reader/writer linked to said redemption station;

whereby said redemption station selects and updates via said at least one smart card reader/writer, coupons stored in a smart card, deleting expired coupons and also those matching purchased items.

8. A system as claimed in claim 7, wherein said system further includes at least one tamper-protected secure coprocessor, whereby operations which assess the validity of coupons including operations which update, collect, store, or delete coupons take place inside said tamper-protected secure coprocessor thereby preventing fraudulent tampering of said coupons.

9. A system as claimed in claim 7, wherein said system further includes at least one issuing station linked to said redemption station, whereby coupons collected by said redemption station are reimbursed by said at least one issuing station.

10. A system as claimed in claim 9, wherein said at least one issuing station includes a database for storing lists of coupons, whereby validation of redeemed coupons are performed by matching said redeemed coupons with said lists of coupons.

11. A method for advertising and issuing at least one coupon electronically, said method comprising:

receiving a request for said electronic coupon from a consumer;

generating at least one electronic advertisement and said electronic coupon;

transmitting said electronic advertisement and said electronic coupon to a consumer's station for presentation to said consumer;

monitoring said consumer's interaction with said advertisement; and

transferring said electronic coupon to a smart card, if said consumer's interaction with said advertisement meets a predefined status.

12. A method as claimed in claim 11, wherein said method further includes the step of retrieving an interest and demographic profile for said consumer before the step of generating.

13. A method as claimed in claim 11, wherein said step of generating includes digitally signing said electronic coupon.

14. A method as claimed in claim 11, wherein said method further includes the steps of:

reading a list of said electronic coupon stored in said smart card;

deleting from said smart card said electronic coupon which have expired;

matching valid said electronic coupon with purchased items; and

extracting valid matching said electronic coupon,

whereby said consumer's electronic coupon is redeemed at a purchasing location when said consumer purchases items associated with said electronic coupon stored in said smart card.

15. The method according to claim 14, wherein said method further includes the steps of:

establishing a connection to an issuing station;

sending said electronic coupon to said issuing station;

validating said electronic coupon; and

reimbursing a merchant for valid said electronic coupon,

whereby said issuing station periodically reimburses merchants collecting said electronic coupon.

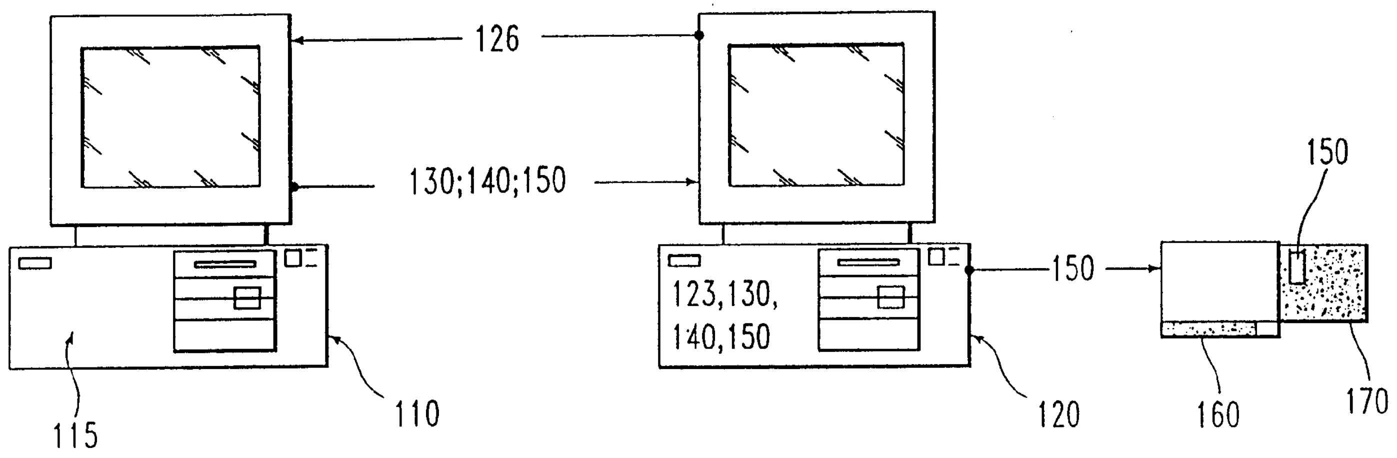


FIG. 1

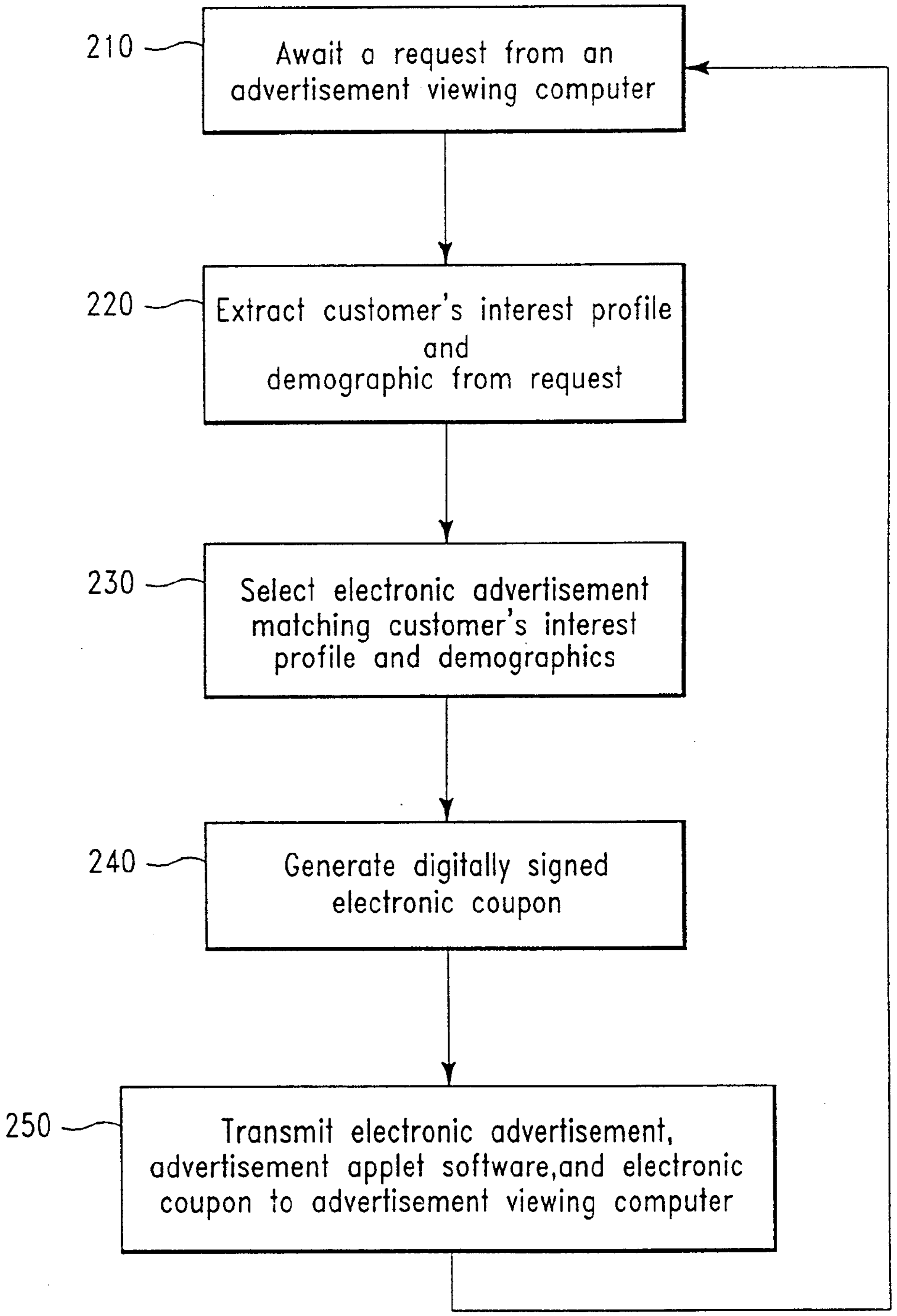

210
Await a request from an advertisement viewing computer
220
Extract customer's interest profile and demographic from request
230
Select electronic advertisement matching customer's interest profile and demographics
240
Generate digitally signed electronic coupon
250
Transmit electronic advertisement, advertisement applet software,and electronic coupon to advertisement viewing computer

FIG. 2

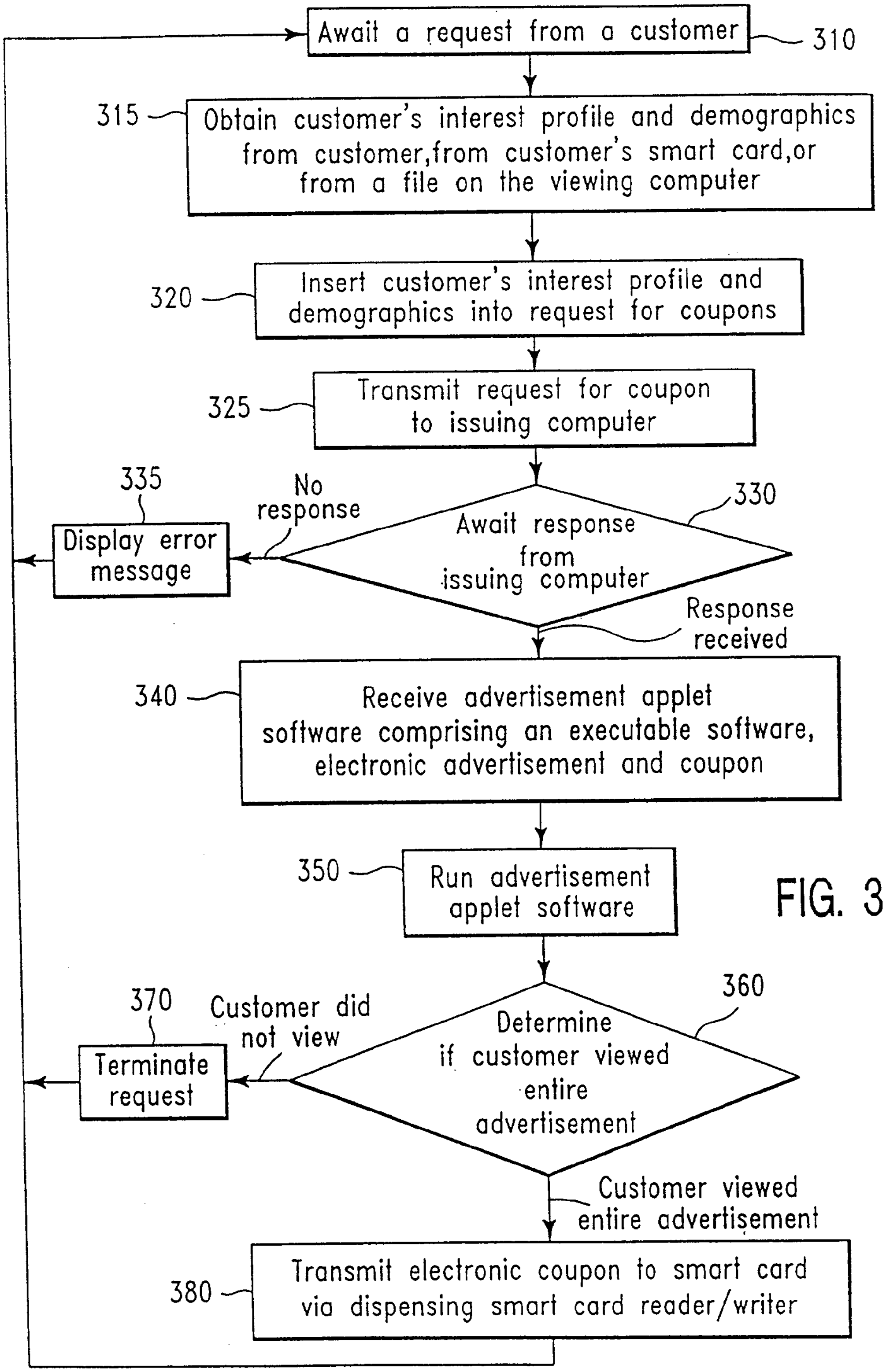

Await a request from a customer
310
315
Obtain customer's interest profile and demographics from customer,from customer's smart card,or from a file on the viewing computer
320
Insert customer's interest profile and demographics into request for coupons
325
Transmit request for coupon to issuing computer
335
Display error message
No response
Await response from issuing computer
330
Response received
340
Receive advertisement applet software comprising an executable software, electronic advertisement and coupon
350
Run advertisement applet software
370
Terminate request
Customer did not view
Determine if customer viewed entire advertisement
360
Customer viewed entire advertisement
380
Transmit electronic coupon to smart card via dispensing smart card reader/writer

FIG. 3

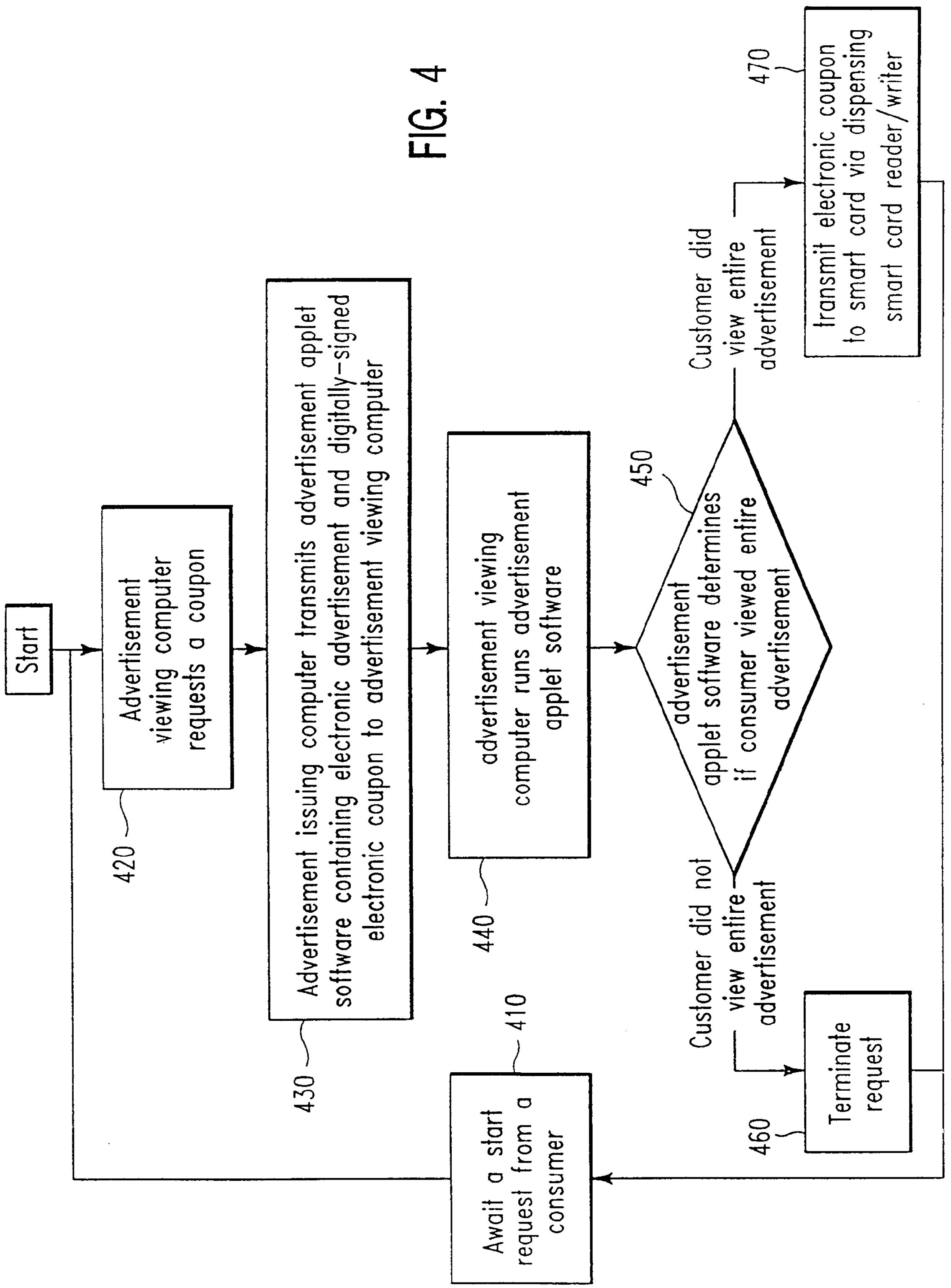

Start
Advertisement viewing computer requests a coupon
420
Advertisement issuing computer transmits advertisement applet software containing electronic advertisement and digitally-signed electronic coupon to advertisement viewing computer
430
advertisement viewing computer runs advertisement applet software
440
advertisement applet software determines if consumer viewed entire advertisement
450
Customer did not view entire advertisement
Customer did view entire advertisement
Terminate request
460
transmit electronic coupon to smart card via dispensing smart card reader/writer
470
Await a start request from a consumer
410

FIG. 4

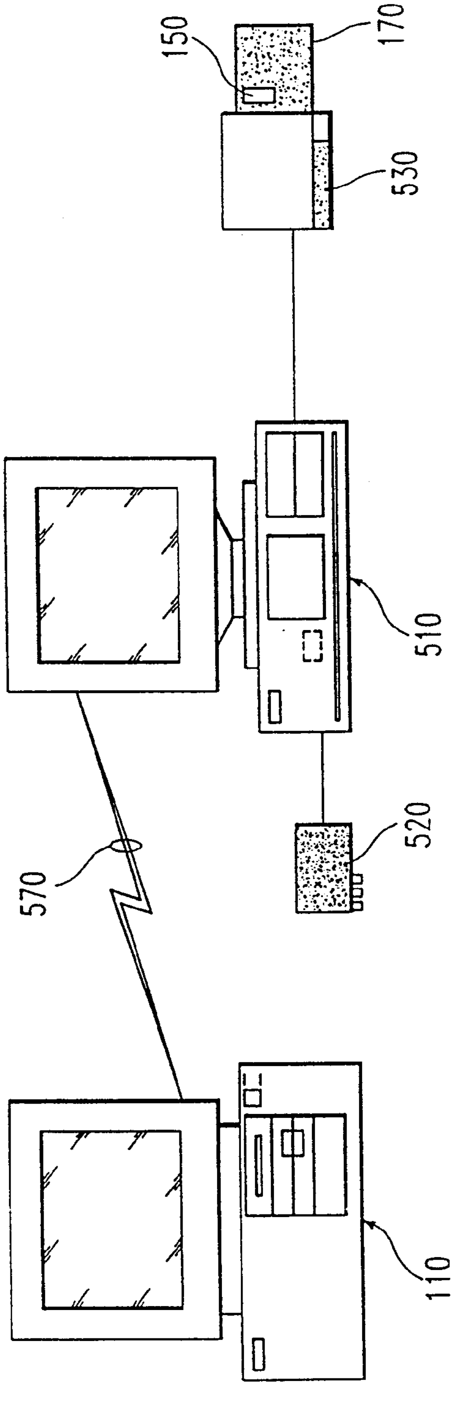


FIG. 5

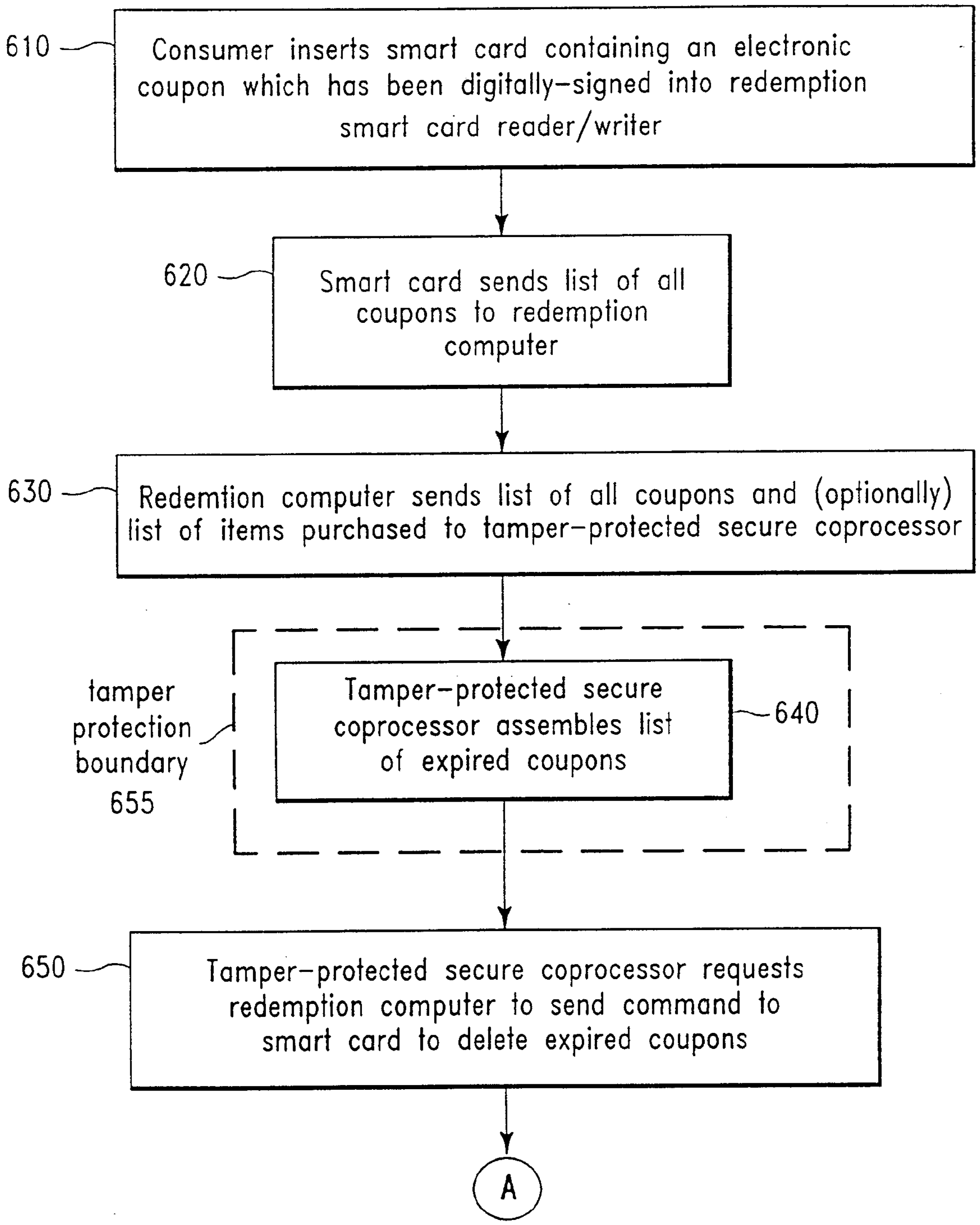

610
Consumer inserts smart card containing an electronic coupon which has been digitally-signed into redemption smart card reader/writer
620
Smart card sends list of all coupons to redemption computer
630
Redemtion computer sends list of all coupons and (optionally) list of items purchased to tamper-protected secure coprocessor
tamper protection boundary 655
Tamper-protected secure coprocessor assembles list of expired coupons
640
650
Tamper-protected secure coprocessor requests redemption computer to send command to smart card to delete expired coupons
A

FIG. 6

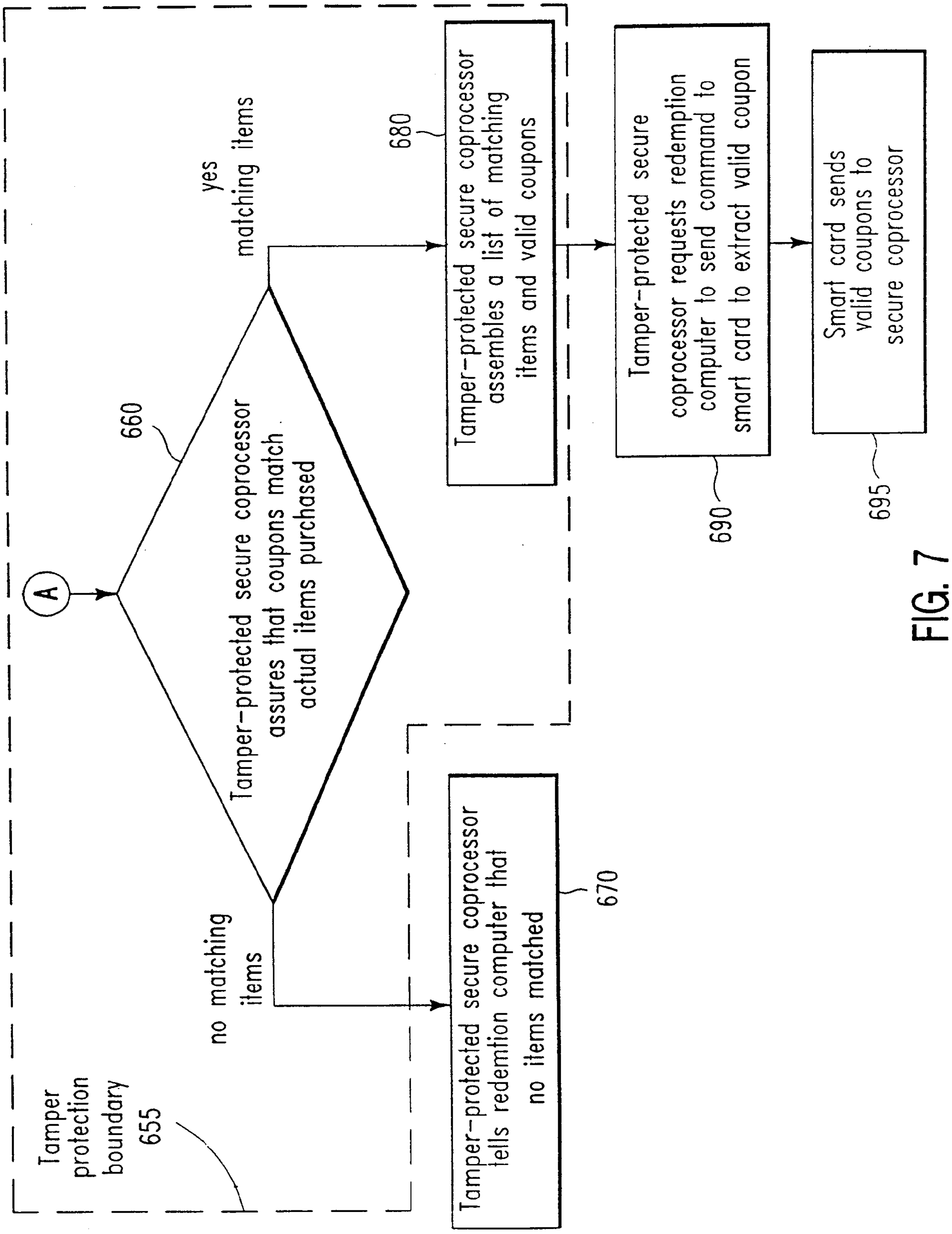

A
Tamper-protected secure coprocessor assures that coupons match actual items purchased
660
yes matching items
680
Tamper-protected secure coprocessor assembles a list of matching items and valid coupons
Tamper-protected secure coprocessor requests redemption computer to send command to smart card to extract valid coupon
690
Smart card sends valid coupons to secure coprocessor
695
no matching items
Tamper-protected secure coprocessor tells redemtion computer that no items matched
670
Tamper protection boundary 655

FIG. 7

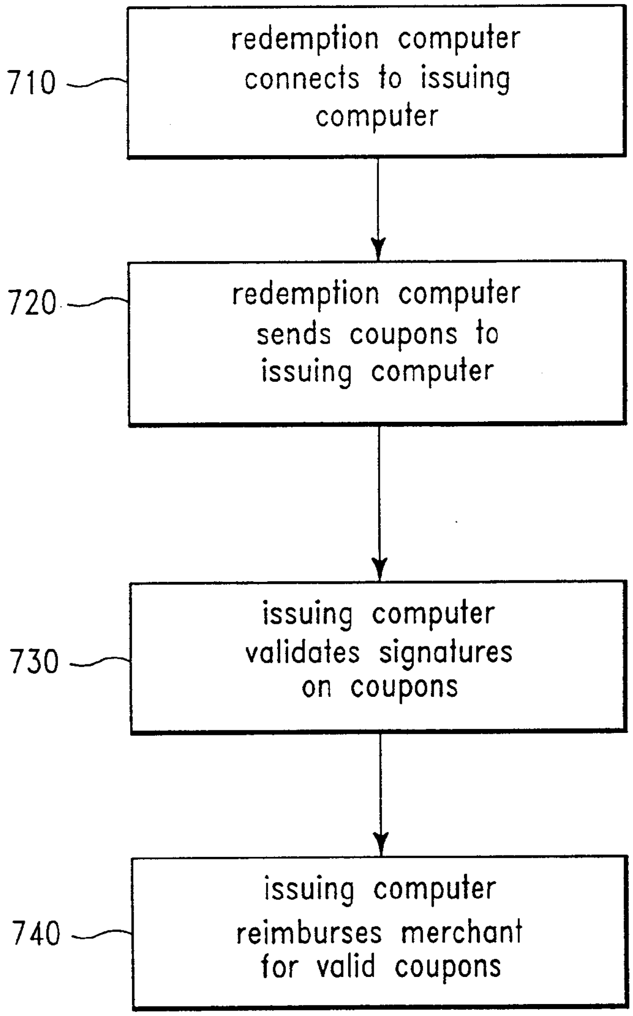

710
redemption computer connects to issuing computer
720
redemption computer sends coupons to issuing computer
730
issuing computer validates signatures on coupons
740
issuing computer reimburses merchant for valid coupons

FIG. 8

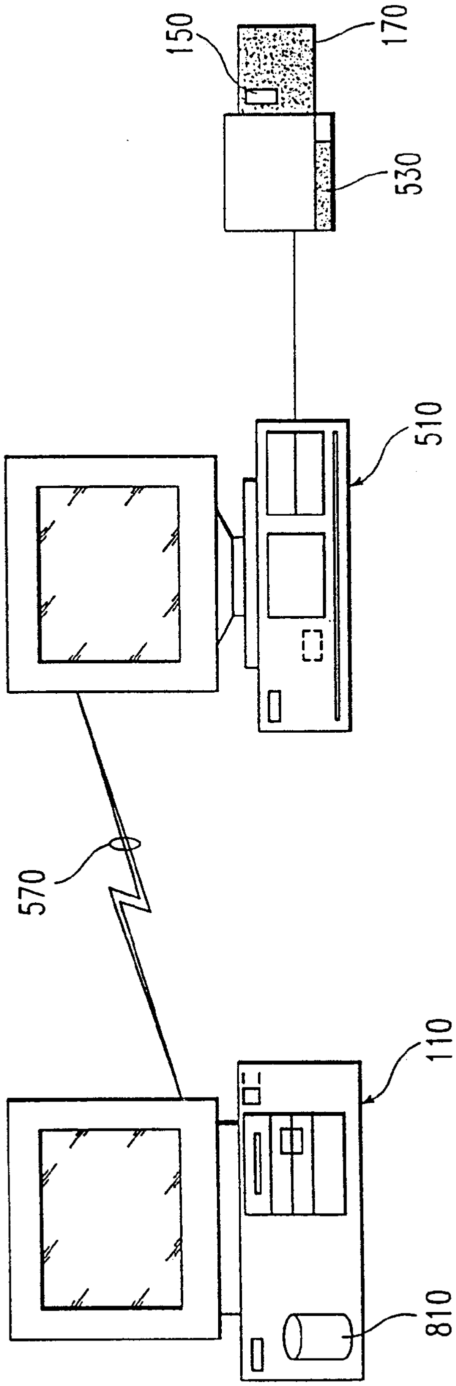


FIG. 9

INTERNATIONAL SEARCH REPORT

Interr ıal Application No
PCT/GB 99/00575

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F17/60 G07F7/02

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F G07F G07G

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	WO 97 30410 A (POWELL KEN R) 21 August 1997 see abstract see page 4, line 15 - line 31 see page 7, line 28 - page 13, line 23 see figures 1,4,5,9,10 ---	1-3 7,11,12
A	US 5 594 493 A (NEMIROFSKY FRANK R) 14 January 1997 see column 3, line 49 - column 6, line 67 see column 11, line 30 - column 12, line 32 see column 13, line 30 - line 43 see column 15, line 21 - line 32 see figure 7 ---	1,2,7
A	US 5 557 721 A (FITE KENNETH R ET AL) 17 September 1996 --- -/--	

☒ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 9 June 1999	Date of mailing of the international search report 16/06/1999
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Bocage, S

1

INTERNATIONAL SEARCH REPORT

Intern   al Application No
PCT/GB 99/00575

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 380 991 A (VALENCIA LUIS ET AL) 10 January 1995 -----	

1

INTERNATIONAL SEARCH REPORT

ormation on patent family members

Interr ıal Application No
PCT/GB 99/00575

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9730410 A	21-08-1997	US 5806044 A	08-09-1998
		AU 2050797 A	02-09-1997
		CA 2246774 A	21-08-1997
US 5594493 A	14-01-1997	AU 683352 B	06-11-1997
		AU 1684395 A	08-08-1995
		CA 2181705 A	27-07-1995
		EP 0761063 A	12-03-1997
		JP 9508993 T	09-09-1997
		WO 9520294 A	27-07-1995
		US 5880769 A	09-03-1999
		US 5767896 A	16-06-1998
US 5557721 A	17-09-1996	WO 9117530 A	14-11-1991
US 5380991 A	10-01-1995	AU 1175195 A	06-06-1995
		WO 9514287 A	26-05-1995

PCT

WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation ^{6} **:**
G06F 1/00

A1

(11) Internationale Veröffentlichungsnummer: **WO 99/38062**

(43) Internationales Veröffentlichungsdatum: 29. Juli 1999 (29.07.99)

(21) Internationales Aktenzeichen: PCT/EP99/00250

(22) Internationales Anmeldedatum: 18. Januar 1999 (18.01.99)

(30) Prioritätsdaten:

198 02 316.2	22. Januar 1998 (22.01.98)	DE
198 41 886.8	11. September 1998 (11.09.98)	DE

(71) Anmelder: KOBIL COMPUTER GMBH [DE/DE]; Weinsheimer Strasse 71, D–67547 Worms (DE).

(72) Erfinder: ISMET, Koyun; Weinsheimer Strasse 71, D–67547 Worms (DE).

(74) Anwalt: REBLE, KLOSE & SCHMITT; Patente + Marken, Postfach 12 15 19, D–68066 Mannheim (DE).

(81) Bestimmungsstaaten: europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Mit internationalem Recherchenbericht.
Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.

(54) Title: METHOD AND DEVICE FOR CREATING PASSWORDS

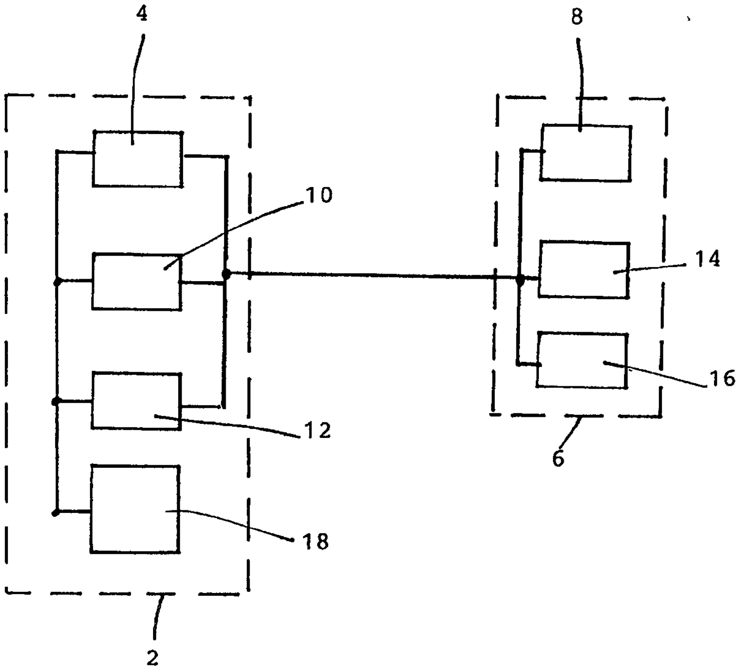
(54) Bezeichnung: VERFAHREN UND VORRICHTUNG ZUR ERZEUGUNG VON PASSWÖRTERN

(57) Abstract

According to the invention, a non–repetitive password is created by both the user and the server. Access is then only permitted when both passwords match.

(57) Zusammenfassung

Einmalpaßwort wird sowohl vom Benutzer als auch vom Server erzeugt. Zugang wird nur dann gewährt, wenn diese beiden Paßwörter übereinstimmen.



LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	**ES**	Spanien	**LS**	Lesotho	**SI**	Slowenien
AM	Armenien	**FI**	Finnland	**LT**	Litauen	**SK**	Slowakei
AT	Österreich	**FR**	Frankreich	**LU**	Luxemburg	**SN**	Senegal
AU	Australien	**GA**	Gabun	**LV**	Lettland	**SZ**	Swasiland
AZ	Aserbaidschan	**GB**	Vereinigtes Königreich	**MC**	Monaco	**TD**	Tschad
BA	Bosnien-Herzegowina	**GE**	Georgien	**MD**	Republik Moldau	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagaskar	**TJ**	Tadschikistan
BE	Belgien	**GN**	Guinea	**MK**	Die ehemalige jugoslawische	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Griechenland		Republik Mazedonien	**TR**	Türkei
BG	Bulgarien	**HU**	Ungarn	**ML**	Mali	**TT**	Trinidad und Tobago
BJ	Benin	**IE**	Irland	**MN**	Mongolei	**UA**	Ukraine
BR	Brasilien	**IL**	Israel	**MR**	Mauretanien	**UG**	Uganda
BY	Belarus	**IS**	Island	**MW**	Malawi	**US**	Vereinigte Staaten von
CA	Kanada	**IT**	Italien	**MX**	Mexiko		Amerika
CF	Zentralafrikanische Republik	**JP**	Japan	**NE**	Niger	**UZ**	Usbekistan
CG	Kongo	**KE**	Kenia	**NL**	Niederlande	**VN**	Vietnam
CH	Schweiz	**KG**	Kirgisistan	**NO**	Norwegen	**YU**	Jugoslawien
CI	Côte d'Ivoire	**KP**	Demokratische Volksrepublik	**NZ**	Neuseeland	**ZW**	Zimbabwe
CM	Kamerun		Korea	**PL**	Polen		
CN	China	**KR**	Republik Korea	**PT**	Portugal		
CU	Kuba	**KZ**	Kasachstan	**RO**	Rumänien		
CZ	Tschechische Republik	**LC**	St. Lucia	**RU**	Russische Föderation		
DE	Deutschland	**LI**	Liechtenstein	**SD**	Sudan		
DK	Dänemark	**LK**	Sri Lanka	**SE**	Schweden		
EE	Estland	**LR**	Liberia	**SG**	Singapur		

Verfahren und Vorrichtung zur Erzeugung von Paßwörtern

Die Erfindung bezieht sich auf ein Verfahren zur Erzeugung von Paßwörtern gemäß den im Oberbegriff des Patentanspruchs 1 angegebenen Merkmalen. Ferner bezieht sich die Erfindung auf eine Vorrichtung zur Durchführung des Verfahrens.

In der Computertechnik gibt es viele Situationen, in denen aus sicherheitstechnischen Gründen eine Authentifizierung eines Benutzers vorgenommen werden muß. Diese Problemstellung ist insbesondere in unsicheren Netzen, wie beispielsweise der Rechnerzugang im Internet oder beim Homebanking via Modem und Telefonnetz von besonderer Bedeutung. Ein potentieller Angreifer darf durch Abhören einer beliebig langen Sequenz von Paßwörtern, welche ein Benutzer oder Client C zur erfolgreichen Berechtigungsüberprüfung oder Authentifizierung beim Server benutzt, nicht in der Lage sein, ein künftiges gültiges Paßwort für den Benutzer oder Client C zu berechnen.

Die Lösung dieser Aufgabe erfolgt gemäß den im Patentanspruch 1 angegebenen Merkmalen sowie gemäß den im Vorrichtungsanspruch angegebenen Merkmalen.

Die erfindungsgemäße Lösung besteht darin, daß der Benutzer dem Rechner ein nur für eine aktuelle Session gültiges Paßwort übergibt, welches ihn eindeutig als den berechtigten Benutzer oder authentischen Client charakterisiert. Der Rechner und insbesondere der Server ist seinerseits in der Lage, das für diesen bestimmten Benutzer aktuell gültige Einmalpaßwort zu bestimmen. Dem Benutzer wird ein weiterer Zugang nur dann gestattet, wenn das eingegebene Paßwort und das vom Rechner berechnete Paßwort übereinstimmen. Wesentlich ist, daß das jeweilige Paßwort immer nur ein einziges Mal gültig ist, welches durch synchrone Berechnung einmalig erzeugt worden ist. Die Sicherheit gegen unbefugte Benutzung ist somit auch in unsicheren Netzen, wie beispielsweise im Internet oder beim Homebanking via Modem und Telefonnetz gewährleistet. Alle Benutzer oder Teilnehmer verwenden das gleiche Verschlüsselungsverfahren oder Kryptosystem, wobei die zugrundeliegende Verschlüsselungsfunktion $f_{k(c)}$ durch einen geheimen Schlüssel k(C) parametrisiert ist. Alle Berechnungen sowohl auf der Benutzerseite als auch auf der Rechnerseite werden in bevorzugter Weise auf einer Prozessorchipkarte durchgeführt, welche zur Durchführung des genannten Verschlüsselungsverfahrens ausgebildet ist. Erfindungsgemäß gelangt eine durch einen geheimen Schlüssel k(C) parametrisierte Schar von Permutationen, d.h. von bijektiven Funktionen auf deren Argumentbereich, $f_{k(C}:D\rightarrow D$ zum Einsatz. Diese Schar genügt wenigstens einer, bevorzugt mehreren der folgenden Bedingungen:

1. Die Definitionsmenge (und Bildmenge) D ist endlich und besitzt hinreichend viele Elemente. Sie enthält insbesondere mindestens 2^{54} viele Elemente.

2. Die Menge aller zulässigen Schlüssel ist hinreichend mächtig. Sie enthält insbesondere mindestens 2^{66} viele Elemente.

3. $f_{k(C)}$ ist eine zufällige Funktion ("random function") in dem Sinne, daß bei beliebigem vorgegebenem Argument x aus der Definitionsmenge D die Wahrscheinlichkeit, ein bestimmtes Element y aus D als Ergebnis der Funktionsauswertung zu erhalten, ungefähr gleich $1/|D|$ ist, wenn man zufällig und gleichverteilt einen Schlüssel k(C) aus der Menge aller möglichen Schlüssel auswählt.

4. Bei Kenntnis einer Folge von Werten x_0, x_1, ..., x_n aus der Definitionsmenge D, wobei $x_{i+1} = f_{k(C)}(x_i)$ für $0\leq i<n$ gelte, soll es einem potentiellen Angreifer in der

Praxis auch mit Hilfe leistungsfähiger Computer unmöglich sein, in vertretbarer Zeit den Schlüssel k(C) zu bestimmen oder $x_{n+1} = f_{k(C)}(x_n)$ zu berechnen.

Der Rechner und der Benutzer verfügen beide über einen geheimen Startwert, welcher Startwert $x_{o,c}$ vom Server initial zufällig erzeugt wird und in einer sicheren Umgebung in den geheimen, von außen nicht zugänglichen Speicherbereich der Chipkarte des Benutzers geschrieben wird. Des weiteren wird mittels des Rechners ein zufälliger geheimer Schlüsselwert k(C) ermittelt und von diesem in einen von außen nicht zugänglicher Speicherbereich eines Datenträgers, insbesondere einer Chipkarte des Benutzers C geschrieben. Die Chipkarte wird dann an den Benutzer C ausgegeben. Des weiteren enthält der Rechner eine nur von Autorisierten zugängliche Datenbank, in welcher die Zuordnung des dem jeweiligen Benutzer zugeordneten geheimen Schlüssels k(C) und das letzte vom Benutzer C benutzte Paßwort $x_{n,c}$ gespeichert ist. Ferner ist in der Chipkarte des Benutzers C in einem gesicherten Speicherbereich dauerhaft der jeweilige geheime Schlüsselwert k(C) sowie das letzte benutzte Paßwort $x_{n,c}$ gespeichert. Des weiteren wird erfindungsgemäß die Benutzung bereits existierender Hard- und Firmware beim Benutzer ermöglicht. So können beispielsweise die bekannten EC-Karten mit Chip benutzt werden, welche als Prozessor-Chipkarten ausgebildet sind und auf welche neben Standardanwendungen, Electronic Cash und elektronische Geldbörse weitere Applikationen nachgeladen werden können. Die von deutschen Banken derzeit ausgegebene EC-Karte vermag standardmäßig folgende Verschlüsselungsverfahren auszuführen: Den Data Encryption Standard, kurz DES, sowie Triple-DES. Des weiteren können die in Mobiltelefonen eingesetzten Chipkarten verwendet werden. Hierbei besitzt ein Benutzer bereits einen geeigneten Chipkartenleser, nämlich sein Mobiltelefon, welches darüber hinaus über ein Display und eine Tastatur verfügt. Weitere Ausgestaltungen und Besonderheiten der Erfindung sind in den Unteransprüchen angegeben.

Die Erfindung wird nachfolgend an Hand des in der Zeichnung dargestelllten Ausführungsbeispiels näher erläutert.

Der Rechner 2 enthält eine erste Einheit 4 zur Durchführung eines bekannten Kryptoverfahrens mit der Verschlüsselungsfunktion $f_{k(c)}$. Der Benutzer erhält einen Datenträger 6, insbesondere in Form einer Chipkarte, welche eine zweite Einheit 8 zur Durchführung des genannten Kryptoverfahrens gemäß $f_{k(c)}$ aufweist. Als Verschlüsselungsverfahren gelangen insbesondere die heute üblichen symmetrischen Kryptosysteme wie DES, Triple-DES oder IDEA zur Verwendung. Anstelle der genannten Verschlüsselungsfunktion $f_{k(c)}$ kann erfindungsgemäß die zugehörige Entschlüsselungsfunktion $f_{k(c)}^{-1}$ verwendet werden. Der Rechner 2 enthält ferner eine erste Kompenente 10 zur Erzeugung eines geheimen Startwertes $x_{0,c}$ sowie eine zweite Komponente 12 zur Erzeugung eines geheimen Schlüssels k(C). Der Datenträger bzw. die Chipkarte 6 enthält einen ersten Speicher 14 für den geheimen Startwert $x_{o,c}$ sowie einen weiteren Speicher 16 für den geheimen Schlüssel k(C). Schließlich enthält der Rechner 2 eine Datenbank 18, welche nur für Autorisierte zugänglich ist und in welcher die Zuordnung des Benutzers bzw. der Chipkarte mit deren geheimen Schlüssel k(C) sowie das letzte vom Benutzer C benutzten Paßwort $x_{n,c}$ gespeichert sind. Alle Benutzer oder Teilnehmer des erfindungsgemäßen Verfahrens oder der erfindungsgemäßen Vorrichtung verwenden das gleiche Kryptosystem mit der gleichen Verschlüsselungsfunktion $f_{k(c)}$ und / oder die zugehörenden Entschlüsselungsfunktion $f_{k(C)}^{-1}$. Es sei festgehalten, daß die Verschlüsselungsfunktion $f_{k(C)}$ eine Permutation, also eine bijektive Funktion auf den Argumentbereich ist, und daß anstelle der genannten Verschlüsselungsfunktion bedarfsweise die zugehörende Entschlüsselungsfunktion verwendbar ist. Die zum Einsatz gelangende Verschlüsselungsfunktion $f_{k(C)}$ ist durch den geheimen Schlüssel k(C) parametrisiert.

Der bevorzugt mittels des Rechners 2 initial zufällig erzeugte geheime Startwert $x_{o,c}$ wird im Rahmen der Erfindung auf den Datenträger 6 in dessen ersten Speicherbereich 14 geschrieben. Ferner wird der bevorzugt gleichfalls mittels des Rechners 2 erzeugte zufällige Schlüssel k(C) in den zweiten von außen gleichfalls nicht zugänglichen Speicherbereich 16 des Datenträgers 6 des Benutzers C geschrieben. Der derart vorbereitete Datenträger bzw. die Chipkarte 6 wird dann dem Benutzer C übergeben und ermöglicht jederzeit dessen Authentifizierung oder Feststellung der Zugriffsberechtigung auf den Rechner 2. Lautet das zuletzt von C benutzte Paßwort $x_{n,c}$, so finden Client C und Server das nächste gültige Paßwort durch Berechnen von

$$x_{n+1,C} = f_{k(C)} (x_{n,\ C}).$$

Im Rahmen der Erfindung ist folglich für den Benutzers mittels des derart vorbereiteten Datenträgers 6 die Möglichkeit geschaffen, dem Rechner jeweils nur für die gewünschte Session ein einmaliges gültiges Paßwort zu übergeben, welches ihn eindeutig als authentischen Benutzer charakterisiert. Der Rechner, insbesondere der Server, ist seinerseits in die Lage versetzt, das für diesen einen Benutzer aktuell gültige Einmalpaßwort zu bestimmen. Ein weiterer Zugang ist für den Benutzer nur dann ermöglicht, wenn das eingegebene Paßwort und das vom Rechner berechnete Paßwort übereinstimmen. Das Einmalpaßwort wird für jede Session oder Transaktion neu erzeugt und ist nur für dieses einzige Mal gültig.

Alternativ kann unter der Voraussetzung, daß die Verschlüsselungsfunktion $f_{k(C)}$ eine Permutation dargestellt, anstelle der Verschlüsselungsfunktion $f_{k(C)}$ die zugehörige Entschlüsselungsfunktion $f_{k(C)}^{-1}$ verwendet werden, wobei die Berechnung des nächsten gültigen Paßworts nach der Formel erfolgt:

$$x_{n+1,C} = f_{k(C)}^{-1} (x_{n,C}).$$

Da ein sicheres Kryptosystem, beispielsweise DES, Triple-DES oder IDEA zum Einsatz gelangt, kenn ein Unbefugter auch bei Kenntnis von $x_{o,C}$ bis $x_{n,C}$ auch das nächste Paßwort $x_{n+1,C}$ nicht berechnen bzw. das Verschlüsselungsverfahren $f_{k(C)}$ nicht berechnen. Durch den Einsatz der genannten heute gängigen symmetrischen Kryptosysteme kann auf die Verwendung der Entschlüsselungsfunktion $f_{k(C)}^{-1}$ anstelle der Verschlüsselungsfunktion $f_{k(C)}$ verzichtet werden, da aus der Kenntnis der expliziten Verschlüsselungsfunktion effizient auf einfache Art und Weise die betreffende Entschlüsselungsfunktion bestimmbar ist.

Damit die Software, welche die Kyptoalgorithmen ausführt, nicht durch Unbefugte manipuliert werden kann, werden in zweckmäßiger Weise die erste Einheit 4, die erste Komponente 10, die zweite Komponente 12 und der zweite Speicherbereich 16 ganz oder teilweise auf einer hochsicheren Prozessorchipkarte realisiert.

Bezugszeichen

2	Rechner
4	erste Einheit
6	Datenträger / Chipkarte
8	zweite Einheit
10	erste Komponente
12	zweite Komponente
14	erster Speicherbereich
16	zweiter Speicherbereich
18	Datenbank

Patentansprüche

1. Verfahren zur Erzeugung von Paßwörtern und zur Überprüfung der Zugriffsberechtigung auf einen Rechner unter Verwendung einer durch einen bevorzugt geheimen Schlüssel k(C) parametrisierte Schar von Permutationen und/oder einer Verschlüsselungsfunktion und eines einem Benutzer zugeordneten Paßworts, dadurch gekennzeichnet, daß ausgehend von einem geheimen Startwert unter Einbeziehung eines zuvor benutzten Paßwortes, insbesondere des zuletzt benutzten Paßwortes, das nächste gültige Paßwort berechnet wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß die durch synchrone Berechnung sowohl im Rechner als auch auf der Benutzerseite erzeugten Paßworte nur einmalig benutzt werden.

3. Verfahren nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die durch den geheimen Schlüssel k(C) parametrisierte Schar von Permutationen, also von bijektiven Funktionen auf deren Argumentbereich, $f_{k(C)}:D \rightarrow D$ zum Einsatz gelangen, die folgenden Bedingungen ganz oder teilweise derart genügt, daß die Definitionsmenge und/oder die Bildmenge D endlich sind und hinreichend viele Elemente, insbesondere mindestens 2^{54} Elemente aufweisen und/oder daß die Menge aller zulässigen Schlüssel hinreichend mächtig ist und bevorzugt mindestens 2^{66} viele Elemente aufweist.

4. Verfahren nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, daß die Funktion $f_{k(C)}$ eine zufällige Funktion (random function) derart ist, daß bei beliebigem vorgegebenem Argument x aus der Definitionsmenge D die Wahrscheinlichkeit, ein bestimmtes Element y aus D als Ergebnis der Funktionsauswertung zu erhalten, ungefähr gleich $1/|D|$ ist, wobei bevorzugt zufällig und/oder gleichverteilt ein Schlüssel k(C) aus der Menge aller möglichen Schlüssel ausgewählt wird.

5. Verfahren nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, daß bei Kenntnis einer Folge von Werten $x_0, x_1, \ldots.., x_n$ aus der Definitionsmenge D, wobei $x_{i+1} = f_{k(C)}(x_i)$ für $0 \leq i < n$ gelte, es einem potentiellen Angreifer in der Praxis auch mit Hilfe leistungsfähiger Computer unmöglich ist, in vertretbarer Zeit den Schlüssel k(C) zu bestimmen oder $x_{n+1} = f_{k(C)}(x_n)$ zu berechnen.

6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß die zugrundliegende Verschlüsselungsfunktion oder Entschlüsselungsfunktion durch den geheimen Schlüsselwert parametrisiert ist.

7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß auf der Rechnerseite eine Zuordnung des geheimen Schlüsselwertes sowie des letzten vom Benutzer genutzten Paßwortes zu diesem Benutzer erfolgt.

8. Verfahren nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, daß die Berechnungen auf der Rechnerseite und / oder auf der Seite des Benutzers durchgeführt werden, vorzugsweise auf einer zur Durchführung des Verschlüsselungsverfahrens ausgelegten Prozessor-Chipkarte.

9. Verfahren nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, daß auf der Benutzerseite, insbesondere auf einer Chipkarte in einem gesicherten Speicherbereich dauerhaft der geheime Schlüsselwert sowie das zuletzt von ihr benutzte Paßwort gespeichert sind.

10. Verfahren nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, daß der geheime Startwert insbesondere mittels des Rechners, initial und zufällig erzeugt wird und in sicherer Umgebung in einem geheimen, von außen nicht zugänglichen Speicherbereich beim Benutzer, insbesondere dessen Chipkarte, gespeichert wird.

11. Verfahren nach einem der Ansprüche 1 bis 10, dadurch gekennzeichnet, daß mittels des Rechners der zufällige, geheime Schlüsselwert erzeugt wird und in einen von außen nicht zugänglichen zweiten Speicherbereich des Benutzers, insbesondere dessen Chipkarte, geschrieben und / oder gespeichert wird.

12. Vorrichtung zur Durchführung des Verfahrens nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, daß der Rechner (2) eine erste Einheit (4) zur Durchführung des Verschlüsselungsverfahrens enthält und / oder eine zweite Einheit (8) zur Erzeugung des geheimen Startwertes enthält.

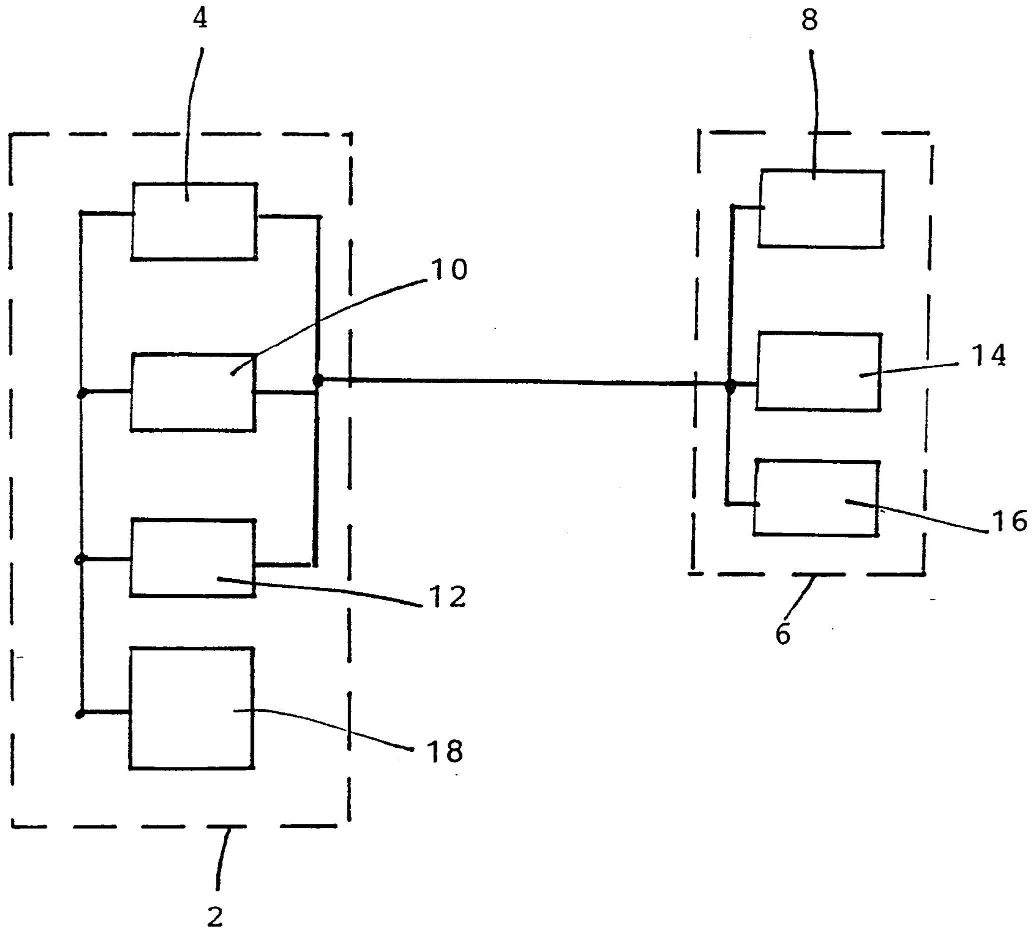
13. Vorrichtung nach Anspruch 12, dadurch gekennzeichnet, daß der Rechner (2) eine erste Speicherkomponente (10) für den geheimen Startwert und / oder eine zweite Speicherkomponente (12) für den Schlüsselwert und / oder eine Datenbank (18) enthält, in welcher eine Zuordnung zum jeweiligen Benutzer erfolgt, und zwar insbesondere

dessen geheimer Schlüsselwert und / oder des letzten vom jeweiligen Benutzer benutzten Paßworts gespeichert ist.

14. Vorrichtung nach einem der Ansprüche 12 oder 13, dadurch gekennzeichnet, daß auf der Benutzerseite ein Datenträger (6), insbesondere eine Chipkarte vorgesehen ist, welche eine zweite Einheit (8) zur Durchführung der Verschlüsselungsverfahrens aufweist.

15. Vorrichtung nach einem der Ansprüche 12 bis 14, dadurch gekennzeichnet, daß der Datenträger bzw. die Chipkarte (6) einen gesicherten ersten Speicherbereich (14) für den geheimen Startwert und / oder einen zweiten gesicherten Speicherbereich (16) für das zuletzt benutzte Paßwort enthält.

16. Vorrichtung nach einem der Ansprüche 12 bis 15, dadurch gekennzeichnet, daß die erste Einheit (4) und/oder die erste Komponente (10) und/oder die zweite Komponente (12) und/oder die Datenbank (18) auf einer hochsicheren Prozessorchipkarte vorgesehen sind.


4
8
10
14
16
12
6
18
2

INTERNATIONAL SEARCH REPORT

Inter. .onal Application No
PCT/EP 99/00250

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 6 G06F F06F G07F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 060 263 A (BOSEN ROBERT J ET AL) 22 October 1991 see figures 1-4,6 see column 5, line 49 - column 9, line 35 ---	1,2,4, 6-10
A	EP 0 262 025 A (FUJITSU LTD) 30 March 1988 see figures 1,2,4,6 see column 2, line 36 - line 56 see column 3, line 18 - column 4, line 50 -----	1,6,8-10

□ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 28 June 1999	Date of mailing of the international search report 06/07/1999
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Weiss, P

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter. onal Application No
PCT/EP 99/00250

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5060263 A	22-10-1991	NONE	
EP 0262025 A	30-03-1988	JP 2086924 C	02-09-1996
		JP 8007720 B	29-01-1996
		JP 63073348 A	02-04-1988
		CA 1298653 A	07-04-1992
		DE 3784824 A	22-04-1993
		DE 3784824 T	11-09-1997
		US 4853522 A	01-08-1989

INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen
PCT/EP 99/00250

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 6 G06F1/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 6 G06F F06F G07F

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	US 5 060 263 A (BOSEN ROBERT J ET AL) 22. Oktober 1991 siehe Abbildungen 1-4,6 siehe Spalte 5, Zeile 49 - Spalte 9, Zeile 35	1,2,4, 6-10
A	EP 0 262 025 A (FUJITSU LTD) 30. März 1988 siehe Abbildungen 1,2,4,6 siehe Spalte 2, Zeile 36 - Zeile 56 siehe Spalte 3, Zeile 18 - Spalte 4, Zeile 50	1,6,8-10

□ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche 28. Juni 1999	Absendedatum des internationalen Recherchenberichts 06/07/1999
Name und Postanschrift der Internationalen Recherchenbehörde Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Bevollmächtigter Bediensteter Weiss, P

1

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP 99/00250

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
US 5060263 A	22-10-1991	KEINE	
EP 0262025 A	30-03-1988	JP 2086924 C	02-09-1996
		JP 8007720 B	29-01-1996
		JP 63073348 A	02-04-1988
		CA 1298653 A	07-04-1992
		DE 3784824 A	22-04-1993
		DE 3784824 T	11-09-1997
		US 4853522 A	01-08-1989

PCT

WELTORGANISATION FÜR GEISTIGES EIGENTUM
Internationales Büro

INTERNATIONALE ANMELDUNG VERÖFFENTLICHT NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT)

(51) Internationale Patentklassifikation 7 : **E05B 49/00, 19/00**	**A1**	**(11) Internationale Veröffentlichungsnummer: WO 00/36252** **(43) Internationales Veröffentlichungsdatum:** 22. Juni 2000 (22.06.00)

(21) Internationales Aktenzeichen: PCT/EP99/09251

(22) Internationales Anmeldedatum: 29. November 1999 (29.11.99)

(30) Prioritätsdaten:
198 58 165.3 16. Dezember 1998 (16.12.98) DE

(71) Anmelder *(für alle Bestimmungsstaaten ausser US)*: HUF HÜLSBECK & FÜRST GMBH & CO. KG [DE/DE]; Steeger Strasse 17, D–42551 Velbert (DE).

(72) Erfinder; und
(75) Erfinder/Anmelder *(nur für US)*: JACOB, Dirk [DE/DE]; Breslauer Strasse 13, D–42579 Heiligenhaus (DE).

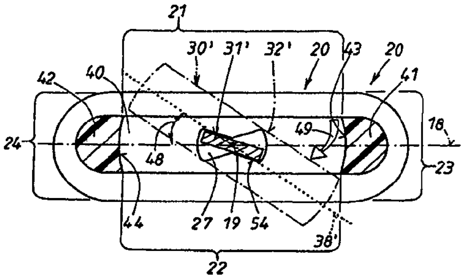
(74) Anwalt: MENTZEL, Norbert; Kleiner Werth 34, D–42275 Wuppertal (DE).

(81) Bestimmungsstaaten: AU, BR, CN, IN, JP, KR, US, europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Veröffentlicht
Mit internationalem Recherchenbericht.

(54) Title: ELECTRONIC KEY, ESPECIALLY FOR MOTOR VEHICLES

(54) Bezeichnung: ELEKTRONISCHER SCHLÜSSEL, INSBESONDERE FÜR KRAFTFAHRZEUGE



(57) Abstract

The invention relates to an electronic key comprising electronic components for receiving or transmitting signals. Said components are integrated in a housing (20). A mechanical emergency key (30') is provided in case of an electronics failure. Said emergency key (30') can be inserted into a recess (27) in the housing (20) together with its key shaft (31'). The aim of the invention is to produce a key which can be handled easily. To this end, one end of the housing is provided with a recess which is undercut at least in places and which usually prevents the inserted emergency key (30') from being pulled out. Usually, the key is in a holding position in the housing (20) with an essentially positive fit. However, the emergency key can be turned in the recess (27) of the housing (20) from a holding position to a release position (30') in which the positive fit between the widening (32') in the key (30') and the recess is eliminated in the pull-out direction of the emergency key.

(57) Zusammenfassung

Bei einem eletronischen Schlüssel sind elektronische Bauteile zum Aussenden bzw. Empfangen von Signalen in ein Gehäuse (20) integriert. Wenn die Elektronik versagt, ist ein mechanischer Notschlüssel (30') vorgesehen, der mit seinem Schlüsselschaft (31') in eine Aufnahme (27) im Gehäuse (20) einsteckbar ist. Um einen bequem zu handhabenden Schlülssel zu entwickeln, wird vorgeschlagen, das eine Gehäuseende mit einem Ausbruch zu versehen, der wenigstens bereichsweise hinterschnitten ist und normalerweise, bei eingestecktem Notschlüssel (30') eine Herausziehbewegung verhindert. Normalerweise befindet sich der Schlüssel in einer im wesentlichen formschlüssigen Haltelage im Gehäuse (20). Der Notschlüssel ist aber in der Aufnahme (27) des Gehäuses (20) aus einer Haltelage in eine Löselage (30') verdrehbar, in welcher der Formschluss zwischen einer Verbreiterung (32') im Schlüssel (30') und dem Ausbruch in Richtung der Herausziehbewegung des Notschlüssels beseitigt ist.

LEDIGLICH ZUR INFORMATION

Codes zur Identifizierung von PCT-Vertragsstaaten auf den Kopfbögen der Schriften, die internationale Anmeldungen gemäss dem PCT veröffentlichen.

AL	Albanien	ES	Spanien	LS	Lesotho	SI	Slowenien
AM	Armenien	FI	Finnland	LT	Litauen	SK	Slowakei
AT	Österreich	FR	Frankreich	LU	Luxemburg	SN	Senegal
AU	Australien	GA	Gabun	LV	Lettland	SZ	Swasiland
AZ	Aserbaidschan	GB	Vereinigtes Königreich	MC	Monaco	TD	Tschad
BA	Bosnien-Herzegowina	GE	Georgien	MD	Republik Moldau	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagaskar	TJ	Tadschikistan
BE	Belgien	GN	Guinea	MK	Die ehemalige jugoslawische Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland			TR	Türkei
BG	Bulgarien	HU	Ungarn	ML	Mali	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MN	Mongolei	UA	Ukraine
BR	Brasilien	IL	Israel	MR	Mauretanien	UG	Uganda
BY	Belarus	IS	Island	MW	Malawi	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	MX	Mexiko		
CF	Zentralafrikanische Republik	JP	Japan	NE	Niger	UZ	Usbekistan
CG	Kongo	KE	Kenia	NL	Niederlande	VN	Vietnam
CH	Schweiz	KG	Kirgisistan	NO	Norwegen	YU	Jugoslawien
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	NZ	Neuseeland	ZW	Zimbabwe
CM	Kamerun			PL	Polen		
CN	China	KR	Republik Korea	PT	Portugal		
CU	Kuba	KZ	Kasachstan	RO	Rumänien		
CZ	Tschechische Republik	LC	St. Lucia	RU	Russische Föderation		
DE	Deutschland	LI	Liechtenstein	SD	Sudan		
DK	Dänemark	LK	Sri Lanka	SE	Schweden		
EE	Estland	LR	Liberia	SG	Singapur		

Elektronischer Schlüssel, insbesondere für Kraftfahrzeuge

Die Erfindung richtet sich auf einen Schlüssel der im Oberbegriff des Anspruches 1 angegebenen Art. Dieser ist nicht nur als elektronischer Schlüssel ausgebildet, sondern umfasst auch einen mechanischen Notschlüssel. Der Notschlüssel dient dazu um bei Ausfall der Elektronik das Schloss mechanisch öffnen zu können.

Bei dem bekannten Schlüssel dieser Art hat das Gehäuse des elektronischen Schlüssels eine Aufnahme für den Notschlüssel. Im Gebrauchsfall lässt sich der Notschlüssel an einer als Schlüsselkopf fungierenden Verbreiterung od. dgl. erfassen. Ein Problem besteht darin, die Einstecklage des Notschlüssels in der Aufnahme zu sichern. Diese Sicherung soll aber nicht die Handhabung des Notschlüssels beim Einstecken und Herausziehen behindern.

Der Erfindung liegt die Aufgabe zugrunde, einen bequem zu handhabenden Schlüssel zu entwickeln, der im Gehäuse im Einsteckfall zuverlässig gehalten wird. Dies wird erfindungsgemäß durch die im Kennzeichen des Anspruches 1 angegebenen Maßnahmen erreicht, denen folgende besondere Bedeutung zukommt.

Die Verbreiterung des Schlüssels dient zweckmäßigerweise auch als Handhabe des Notschlüssels und besteht in der Regel aus einen Schlüsselkopf. Es versteht sich, dass eine solche Verbreiterung nicht die Funktion der Handhabe vom Notschlüssel haben muss. Der Einfachheit wegen soll nachfolgend diese Verbreiterung aber stets mit „Schlüsselkopf" bezeichnet werden. Bezüglich des Gehäuses lässt sich der Schlüsselkopf zwischen zwei zueinander drehversetzten Lagen überführen, nämlich einer seine Position im Gehäuse sichernden Haltelage und einer seine Entnahme aus dem Gehäuse ermöglichenden Löselage. In der Haltelage liegt ein Formschluss vor, wo die Verbreiterung bzw. der Schlüsselkopf wenigstens bereichsweise in einem Ausbruch des einen Gehäuseendes sich befindet. In der Haltelage ist ein Herausziehen des Notschlüssels aus dem Gehäuse nicht möglich. Das Herausziehen ist aber schnell und bequem ausführbar, weil der Schlüsselkopf in einer im wesentlichen senkrecht zur Ebene des Ausbruchs liegenden Richtung nicht vom Gehäuse überdeckt ist und in die demgegenüber verdrehte Löselage bewegt werden kann. Diese Bewegung erfolgt als Drehung um eine in Längsrichtung des Schlüsselschafts verlaufende Drehachse. In der Löselage ist der Schlüsselkopf nicht mehr formschlüssig erfasst. Dann ist eine translatorische Bewegung des Notschlüssels im Sinne eines Herausziehens möglich. Das Herausziehen des Notschlüssels aus dem Gehäuse in der Löselage erfolgt also in einer drehversetzten Ebene bezüglich der vorausgehend in der Haltelage bestehenden Position zwischen Gehäuse und Schlüsselkopf.

Diese Bewegung der Bauteile beim Kuppeln und Entkuppeln lässt sich als „Einrenkbewegung" beschreiben. Die Verbreiterung des Schlüssels bzw. der zu seiner Handhabung dienende Schlüsselkopf können eine ausreichend große Fläche aufweisen, ohne die Sicherungsfunktion in der Haltelage zu gefährden. Dadurch ist die Handhabung sowohl beim Kuppeln als auch Entkuppeln und schließlich bei der Schlüsselbetätigung erleichtert. Dies gilt insbesondere wenn man den Schlüsselkopf und das Gehäuse plattenartig ausbildet, die in der Haltelage einen bündigen Übergang der Außenflächen dieser Bauteile gewährleisten. Störende Kanten oder Vorsprünge liegen nicht vor. Daher ist die Aufbewahrung des Schlüssels in der Hosentasche der Bedienungsperson besonders angenehm.

Weitere Maßnahmen und Vorteile der Erfindung ergeben sich aus den Unteransprüchen, der nachfolgenden Beschreibung und den Zeichnungen. In den Zeichnungen ist die Erfindung in einem Ausführungsbeispiel dargestellt. Es zeigen:

Fig. 1 eine Draufsicht auf das Gehäuse des elektronischen Schlüssels mit eingestecktem Notschlüssel,

Fig. 2, schematisch, einen Längsschnitt durch das Gehäuse von Fig. 1,

Fig. 3 + 4 zwei Querschnitte durch das Gehäuse von Fig. 1 und 2 längs der Schnittlinien III - III bzw. IV - IV,

Fig. 5, in einer der Fig. 4 entsprechenden Darstellung, die Lage der Bauteile von Fig. 4 in einer anderen, drehversetzten Lage,

Fig. 6, in einer der Fig. 2 entsprechenden Darstellung, nachdem der Notschlüssel aus dem Gehäuse entnommen worden ist,

Fig. 7, in Draufsicht, den aus dem Gehäuse entnommenen Notschlüssel und

Fig. 8, in perspektivischer, gestreckter Position eine flexible Leiterplatte zur Aufnahme elektronischer Bauteile, die in gefaltetem Zustand im Gehäuse untergebracht wird.

Der erfindungsgemäße Schlüssel umfasst eine Kombination aus dem eigentlichen elektronischen Schlüssel 10 und einem mechanischen Notschlüssel 30. Der elektronische Schlüssel 10 kann über eine größere Entfernung auf ein nicht näher gezeigtes, an ein Kraftfahrzeug angeordnetes Schloss durch codierte Signale 15 wirken. Dazu besitzt das Gehäuse 20, das aus mehreren Gehäuseteilen 21 bis 24 zusammengesetzt sein kann, geeignete elektronische Bauteile 11 und

Betätigungsstellen 13, 14, die dieses Signal 15 generieren und, gegebenenfalls im Dialog, an die entsprechende komplementäre Sende- und Empfangseinrichtung im Fahrzeug weiterleiten. Im Erfolgsfall, wenn die Codierung der Signale 15 akzeptiert wird, wird ein nicht näher gezeigtes elektronisches oder elektromechanisches Schloss wirksam gesetzt. Im Bereich dieser Betätigungsstellen 11 bis 14 sind Mikroschalter 17 angeordnet, die aus Fig. 8 erkennbare Schaltglieder 62 aufweisen. Diese sitzen, zusammen mit den Bauteilen 11 auf einer vorzugsweise auch elektrische Leiterbahnen aufweisende Folie 60, die in Fig. 8 gezeigt ist. Diese Folie 60 kann stellenweise Dellen 61 aufweisen, in welchen manche der Elemente 11 bzw. Glieder 62 versenkt angeordnet sind. Die Folie 60 lässt sich falten und in einen mehr oder weniger zylindrischen Raum im Inneren des Gehäuses 20 unterbringen. Das Gehäuse 20 ist längssymmetrisch aufgebaut bezüglich seiner in Fig. 1 dargestellten Längsmitte 16. Das Gehäuse 20 ist plattenförmig gestaltet, wie aus 63 in Fig. 4 zu ersehen ist und bestimmt eine in Fig. 4 strichpunktiert angedeutete Mittenebene 18.

Der grundsätzliche Aufbau des Notschlüssels 30 ergibt sich aus Fig. 7. Diese umfasst den Schlüsselschaft 31 mit nicht näher gezeigten profilierten Einschnitten bzw. Bahnen für entsprechende Steuermittel im Schloss. An seinem äußeren Ende befindet sich eine Verbreiterung, die einstückig oder mehrstückig gegenüber dem Schlüsselschaft 31 sein kann. Im vorliegenden Fall besteht sie aus einem Schlüsselkopf 32 aus Kunststoff. Der Schlüsselschaft 31 besitzt ein Flachprofil 50, das vorzugsweise aus Metall besteht. Auch der Schlüsselkopf 32 bestimmt eine durch die Punktlinie 38 in Fig. 4 verdeutlichte Mittenebene 38. Das Flachprofil 50 des Schlüsselschafts 31 ist, wie aus Fig. 4 hervorgeht, gegenüber dem vorzugsweise symmetrischen Querschnittsprofil des Schlüsselkopfs 32, ausweislich der strichpunktiert eingezeichneten Querschnittsebene 50 um einen Winkel 39 bezüglich dieser Mittenebene 38 verkippt. Sowohl der Umriss des Gehäuses 20 als auch der des Schlüsselkopfes 32 sind zwar plattenartig 63, 64, gemäß Fig. 4, ausgebildet, können aber in sich profiliert sein. Normalerweise befindet sich der Notschlüssel 30 in seiner aus Fig. 1 bis 4 gezeigten Ruheposition, die nachfolgend kurz „Haltelage“ des Notschlüssels bezeichnet werden soll. In diesem Fall liegt die Mittenebene 18 des

Gehäuses 20 im wesentlichen höhengleich mit der Mittenebene 38 des Schlüsselkopfs 32.

Wie am besten aus Fig. 6 zu entnehmen ist, besitzt das hintere Gehäuseende 28 einen Ausbruch 40, der hier als Gabelöffnung ausgebildet ist. Dadurch entstehen den Ausbruch 40 begrenzende Gabelschenkel 41, 42. Die den Ausbruch 40 nach innen begrenzende Endwand 26 ist mit einer Aufnahme 27 für den bereits beschriebenen Schlüsselschaft 31 des Notschlüssels 30 versehen, wenn die Haltelage 30 gemäß Fig. 1 bis 4 vorliegt. Die Aufnahme 27 entsteht hier durch einen mit der Endwand 26 einstückigen Köcher 25, der einen Innengehäuse bildet und sich in diesem Ausführungsbeispiel in der bereits genannten Längsmitte 16 des Gehäuses 20 befindet. In der Haltelage gemäß Fig. 1 bis 4 ist der Notschlüssel 30 in seiner Einstecklage in der Aufnahme 27 zunächst gesichert und lässt sich nicht ohne weiteres im Sinne des Pfeils 47 von Fig. 2 herausziehen. Dazu werden folgende besondere Maßnahmen vorgeschlagen.

Der Ausbruch 40 ist wenigstens stellenweise bei 43, 44 hinterschnitten. Im vorliegenden Fall wird dies an den beiden Schenkeln 41, 42 durch mehr oder weniger konvergent aufeinander zu laufende Innenflächen 43, 44 der beiden Schenkel 41, 42 erreicht. Dadurch kommt es wenigstens punktuell zu einem Formschluss zwischen den einen Hinterschnitt 45, 46 gemäß Fig. 6 erzeugenden Schenkeln 41, 42 einerseits und dem Schlüsselkopf 32 andererseits. In dieser Haltelage befindet sich der Schlüsselkopf 32 in einer möglichst bündigen Position zum Gehäuse 20, wie durch die bereits erwähnte übereinstimmende Höhenlage der Mittenebene 18, 38 der beiden Plattenformen 63, 64 von Fig. 4 zu entnehmen ist. Zur zusätzlichen Sicherung der Haltelage von Fig. 1 bis 4 können an den Berührungsstellen der Schenkel 41, 42 und im Umfangsbereich zusammenwirkende Rastelemente 51, 52 vorgesehen sein, z.B. ein Vorsprung 51 und eine Vertiefung 52, wie aus Fig. 3 und 5 zu entnehmen ist. Es ist eine Art Einrenkverbindung erforderlich, um den Notschlüssel 30 aus dem Gehäuse 20 im Sinne des Pfeils 47 herausziehen zu können. Dies soll anhand der Fig. 5 näher erläutert werden.

Die Aussparung 40 im Gehäuse 20 ist nach oben bzw. unten offen, weshalb eine Drehung des Schlüsselkopfes aus seiner Haltelage im Sinne des Pfeils 49 der Fig. 3 bis 5 möglich ist. Diese Drehung erfolgt um eine Drehachse 19, die im vorliegenden Fall mit der erwähnten Gehäuselängsmitte 16 zusammenfällt. Man erreicht so die aus Fig. 5 erkennbare andere Lage der Bauteile 20, 30', die aus guten Gründen nachfolgend als „Löselage" des Notschlüssels bezeichnet werden soll. In dieser Löselage 30' liegt nicht mehr der vorgeschriebene Formschluss vor. Jetzt lässt sich der Notschlüssel 30' im Sinne der bereits mehrfach erwähnten Pfeile 47 herausziehen. Eine Kollision der Bauteile 20, 30' findet dann nicht mehr statt. Die vorerwähnte Drehung 49 kann durch Endanschläge 53, 54 im Inneren der Aufnahme 27 begrenzt sein. Im vorliegenden Fall ist der Kippwinkel 39 von Fig. 4 etwa nur halb so groß wie der Drehwinkel 48, bezogen auf die Mittenebene 16 vom Gehäuse 20.

Gemäß Fig. 1 ist der Notschlüssel 30 mit einem überraschend großen Schlüsselkopf 32 versehen, der, zwecks besserer Deutlichkeit, in Punktschraffur dargestellt ist. Das lässt eine bequeme Handhabung sowohl bei der vorbeschriebenen Entnahme 47 als auch bei der späteren Drehbetätigung des Notschlüssels 30 im Schloss zu. Der Schlüsselkopf 32 kann sogar mit einem Reststück 59 über die äußerste Begrenzung des Gehäuses 10 an den Enden der beiden Schenkel 41, 42 in der Haltelage herausragen.

Der Formschluss zwischen der Aussparung 40 und dem Notschlüssel 40 kommt also bei der Erfindung durch axiale Abstützung und gegebenenfalls durch radiale Drehanschläge im Bereich des Schlüsselkopfs 32 zustande. Statt des Schlüsselkopfs 32 könnten auch Verbreiterungen im Schlüsselschaft 31 od. dgl. genutzt werden. Günstig ist es hier für eine Flächenberührung zu sorgen, weshalb die vorbeschriebenen Innenflächen 43, 44 der beiden Schenkel 41, 42 der Drehung 49 entsprechende Rundungen aufweisen und mit möglichst engen Fugen mit einem entsprechenden Gegenprofil bei 33, 34 des Schlüsselkopfs 32 zu liegen kommen. Im vorliegenden Fall sind die beiden einander gegenüberliegenden Kopfseitenflächen 33, 34 im Sinne der Hilfslinien 35, 36 von Fig. 7 in Richtung auf das freie Kopfende 37 sich im wesentlichen linear verjüngt. Dazu ergibt sich ein Formschluss durch Flächenberührung zwischen 33, 43 einerseits und 34, 44 andererseits. Wegen der Drehung 49 zum Entkuppeln und, wie sich zeigen wird, auch beim Kuppeln, könnte aber der Hintergriff der Bauteile 20, 30 in der Haltelage auch an anderen Stellen wirksam werden, z.B. am freien Kopfende 37. Wegen des guten Hintergriffs lässt sich der in der Haltelage befindliche Notschlüssel 30 auch durch große axiale Kräfte im Sinne der Herausziehpfeils 47 nicht entfernen. Der Notschlüssel ist in seiner Haltelage 30 so zuverlässig in seinem Ausbruch 40 gegenüber im Herausziehsinne wirkende Kräfte positioniert, dass sein Schlüsselkopf 32 ohne weiteres mit einem Aufhängeloch 56 für Schlüsselanhänger od. dgl. versehen sein kann.

Die vorbeschriebene Einrenkbewegung findet im umgekehrten Sinne statt, wenn man, ausgehend von einem entnommenen Notschlüssel wieder in die Aussparung des Gehäuses 20 von Fig. 6 im Sinne des Pfeils 58 von Fig. 6 in das Gehäuse 20 einstecken will. In diesem Fall befindet sich der Notschlüssel zunächst in seiner Löselage 30‘ außerhalb des Gehäuses 20 und wird dann, im Sinne des Pfeils 58 von Fig. 6, in die Aufnahme 27 hineingeschoben, bis durch axiale Anschläge die Endposition erreicht ist. Dann wird der Notschlüssel in Gegenrichtung zum Drehpfeil 49 in seine Haltelage 30 von Fig. 3 bzw. 4 zurückgeführt.

Das Gehäuse 20 besteht, wie bereits erwähnt wurde, aus mehreren Gehäuseteilen 21 bis 24. Sie umfassen eine im mittleren Bereich angeordnete Oberschale 21 und Unterschale 22 und zwei Seitenteile 23, 24. Die Seitenteile werden von Nocken 57 od. dgl. durchgriffen, die an der Ober- bzw. Unterschale 21, 22 sitzen und für einen Zusammenhalt dieser Gehäuseteile sorgen. Der Ausbruch 40 erfolgt durch Verlängerungen der Gehäuseseitenteile 23, 24 über das Ende der Ober- und Unterschale 21, 22 hinaus, wodurch die bereits erwähnten Gabelschenkel 41, 42 entstehen. Das vordere Gehäuseende 29 wird von der zusammengefügten Ober- und Unterschale 21, 22 gebildet und weist bei 65 von Fig. 2 eine stumpfe Form auf. An diesem vorderen Gehäuseende 29 beginnen die beiden Seitenteile 23, 24 in einem Axialabstand 66 gegenüber der stumpfen Front 65.

Bezugszeichenliste:

10	elektronischer Schlüssel
11	elektronische Bauteile
12	erste Betätigungsstelle von 10
13	zweite Betätigungsstelle von 10
14	dritte Betätigungsstelle von 10
15	Signal von 10
16	Gehäuselängsrichtung, Längsmitte
17	Mikroschalter
18	Mittelebene von 20, Gehäuseebene
19	Drehachse für 30 in 30‘
20	Gehäuse, Gesamtgehäuse
21	Oberschale von 20
22	Unterschale von 20
23	erster Seitenteil von 20
24	zweiter Seitenteil von 20
25	Köcher für 31 in 20
26	Endwand von 25 zwischen 21, 22
27	Aufnahme in 25 für 31
28	hinteres Gehäuseende von 20
29	vorderes Gehäuseende von 20
30	Notschlüssel (Haltelage; gesichert)
30‘	Löselage von 30
31	Schlüsselschaft von 30 (Haltelage)
31‘	Löselage von 31 bei 30‘
32	Schlüsselkopf von 30 (Haltelage)
32‘	Löselage von 32
33	Gegenprofil für 43 an 32 (Fig. 7), erste Kopfseitenfläche von 32
34	Gegenprofil für 44 an 32 (Fig. 7), zweite Kopfseitenfläche von 32

35	Verjüngung von 33
36	Verjüngung von 34
37	freies Kopfende von 32
38	Ebene des Schlüsselkopfs, Mittenebene von 32 (in Haltelage, Fig. 4)
38‘	Löselage von 38 (Fig. 5)
39	Kippwinkel zwischen 31, 38
40	Ausbruch in 28, Gabelöffnung
41	erster Schenkel von 23, Gabelschenkel
42	zweiter Schenkel von 24, Gabelschenkel
43	Innenfläche von 41
44	Innenfläche von 42
45	Winkel des Hinterschnitts von 43
46	Winkel des Hinterschnitts von 44
47	translatorischer Herauszieh-Pfeil von 30‘
48	Drehwinkel zwischen 30, 30‘
49	Drehpfeil von 30
50	Flachprofil von 31
51	erstes Rastelement an 33, 34, Vorsprung
52	zweites Rastelement an 43, 44, Vertiefung
53	erster Drehanschlag in 27 für 31
54	zweiter Drehanschlag in 27 für 31‘
55	Ebene von 50
56	Aufhängeloch in 32 (Fig. 7)
57	seitlicher Nocken an 22 bzw. 21 für 23 bzw. 24
58	translatorischer Pfeil der Einsteckbewegung von 30‘ (Fig. 6)
59	herausragendes Reststück von 32 (Fig. 1)
60	Folie in 12 und 17
61	Delle in 60 für 17
62	Schaltglied an 17 (Fig. 8)
63	Plattenform von 20 (Fig. 4)
64	plattenartige Form von 32 (Fig. 4)

65	stumpfe Front von 29
66	Axialabstand von 23, 24 gegenüber 29 (Fig. 1)

Patentansprüche:

1.) Elektronischer Schlüssel (10), insbesondere für Kraftfahrzeuge, mit einem Gehäuse (20), das elektronische Bauteile (11) aufnimmt und zum Aussenden bzw. Empfangen von Signalen (15) zum Wirksamsetzen eines zugehörigen elektronischen oder elektromechanischen Schlosses beinhaltet,

mit einem mechanischen Notschlüssel (30), der mit seinem Schlüsselschaft (31) in eine Aufnahme (27) des Gehäuses (20) einsteckbar und im Einsteckfall im Gehäuse gesichert ist, wobei der Notschlüssel (30) mit einer Verbreiterung (32) versehen ist,

dadurch gekennzeichnet,

dass das eine Gehäuseende (28) einen Ausbruch (40) aufweist, der wenigstens bereichsweise hinterschnitten (45, 46) ist und normalerweise, bei eingestecktem Notschlüssel (30) seine Herausziehbewegung (47) verhindert,

wobei der Schlüsselkopf sich in einer im wesentlichen formschlüssigen Haltelage (30) im Gehäuse (20) befindet

und dass der Notschlüssel in der Aufnahme (27) des Gehäuses (20) aus dieser Haltelage (30) in eine Löselage (30‘) verdrehbar ist, in welcher der Formschluss zwischen der Verbreiterung (32‘) und dem Ausbruch (40) in Richtung der Herausziehbewegung (47) des Notschlüssels beseitigt ist.

2.) Schlüssel nach Anspruch 1, dadurch gekennzeichnet, dass die Verbreiterung im Notschlüssel (30) aus der zur Schlüsselbetätigung dienenden Handhabe, wie einem Schlüsselkopf (32), besteht.

3.) Schlüssel nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass der Ausbruch (40) wenigstens auf seiner einen Seite von einem Schenkel (41; 42) begrenzt ist und der Schenkel (41; 42) auf der dem Ausbruch (40) zugekehrten Innenflanke (43; 44) den Hinterschnitt (45; 46) aufweist

und dass der Schlüsselkopf (32) mit seiner der Innenflanke (43; 44) vom Gehäuseschenkel (41, 42) zugekehrten Kopfseitenfläche (33; 34) sich zum freien Kopfende (37) hin mindestens bereichsweise verjüngt und in der Haltelage (30) des Notschlüssels sich mindestens stellenweise am Gehäuseschenkel (41; 42) abstützt.

4.) Schlüssel nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass der Schlüsselkopf (32) und das Gehäuse (20) plattenartig (63; 64) ausgebildet sind, wobei die Plattenform jeweils zwei Mittenebenen (18, 38) bestimmt,

und dass die Mittenebene (18, 38) in der Haltelage zwar im wesentlichen miteinander fluchten, aber in der Löselage die beiden Ebenen (18, 38‘) zueinander drehversetzt (48) sind.

5.) Schlüssel nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass zwischen dem Schlüsselkopf (32) und dem Ausbruch (40) im Gehäuse (30) Rastelemente angeordnet sind, welche die Haltelage (30) gegenüber Drehungen (49) sichern.

6.) Schlüssel nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, dass in der Aufnahme des Gehäuses Drehanschläge (53; 54) vorgesehen sind, welche die Position des Schlüsselschafts in der Haltelage (31) und/oder der Löselage (31') bestimmen und die Drehung (49) des Schlüsselschafts zwischen diesen beiden Lagen (31; 31') begrenzen.

7.) Schlüssel nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass der Schlüsselschaft (31) ein Flachprofil (50) aufweist,

dass der Schlüsselkopf (32) des Notschlüssels (30) ein vorzugsweise symmetrisches Querschnittsprofil besitzt, welches die Mittenebene (38) im Schlüsselkopf (32) bestimmt,

und dass die Ebene (55) vom Flachprofil (50) des Schlüsselschafts (31) gegenüber der Mittenebene (38) im Schlüsselkopf (32) gegenüber jener Drehachse (19) verkippt (39) ist, welche die Drehung (49) des Notschlüssels zwischen der Haltelage (30) und der Löselage (30') bestimmt.

8.) Schlüssel nach Anspruch 7, dadurch gekennzeichnet, dass der Kippwinkel (39) zwischen der Flachprofilebene (55) des Schlüsselschafts (31) und der Mittenebene (38) vom Schlüsselkopf (32) annähernd gleich dem halben Drehwinkel (48) des Schlüsselschafts zwischen dessen Ruhelage (31) und Löselage (31') ist.

9.) Schlüssel nach einem oder mehreren der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass die Aufnahme (27) für den Schlüsselschaft (31) im Gehäuse aus einem Köcher (25) eines Innengehäuses besteht.

10.) Schlüssel nach Anspruch 9, dadurch gekennzeichnet, dass das Innengehäuse zwischen einer Oberschale (21) und einer Unterschale (22) eines mehrteiligen Gesamtgehäuses (20) angeordnet ist.

11.) Schlüssel nach einem der Ansprüche 1 bis 10, dadurch gekennzeichnet, dass der Schenkel (41, 42) des Ausbruches (40) aus dem Endstück eines den Längsrand des Gesamtgehäuses (20) erzeugenden Gehäuseseitenteils (23) bzw. (24) gebildet wird.

12.) Schlüssel nach Anspruch 11, dadurch gekennzeichnet, dass seitliche Nocken (57) od. dgl. die Ober- und Unterschale (21, 22) des Gesamtgehäuses (20) mit dem bzw. den Gehäuseseitenteilen (43; 24) verbinden.

13.) Schlüssel nach einem der Ansprüche 1 bis 12, dadurch gekennzeichnet, dass die Aufnahme (27) im wesentlichen in der Längsmitte (16) des Gehäuses (20) angeordnet ist

und dass die Längsmitte (16) eine Symmetrieachse des Gehäuses (20) bestimmt.

14.) Schlüssel nach einem der Ansprüche 1 bis 13, dadurch gekennzeichnet, dass das hintere Gehäuseende (28) gegabelt (40) ist und

dass der Ausbruch im Gehäuse (20) aus einer Gabelöffnung (40) besteht, die beidseitig von zwei sie begrenzenden Gabelschenkeln (41; 42) eingefasst ist.

15.) Schlüssel nach Anspruch 14, dadurch gekennzeichnet, dass die beiden Gabelschenkeln (41; 42) an ihren einander zugekehrten Innenflanken (43; 44) jeweils einen zueinander gegensinnigen Hinterschnitt (45; 46) für den Schlüsselkopf (32) des Notschlüssels (30) aufweisen.

16.) Schlüssel nach einem der Ansprüche 1 bis 15, dadurch gekennzeichnet, dass die elektronischen Bauteile (11) auf einer als flexibe Leiterplatte dienenden Folie (60) sitzen

und dass, - im Querschnitt gesehen -, diese Folie (60) in einer C-artigen Krümmung um die in Gehäuselängsrichtung (16) sich erstreckende Aufnahme (27) verläuft.

17.) Schlüssel nach Anspruch 16, dadurch gekennzeichnet, dass die Folie (60) stellenweise Dellen (61) aufweist, in denen Mikroschalter (17) positioniert sind,

und dass die Schaltglieder (62) an den Mikroschaltern (17) bei gekrümmter Folie (60) mit den Betätigungsstellen (12, 13, 14) auf der Außenseite des Gehäuses (20) ausgerichtet sind.

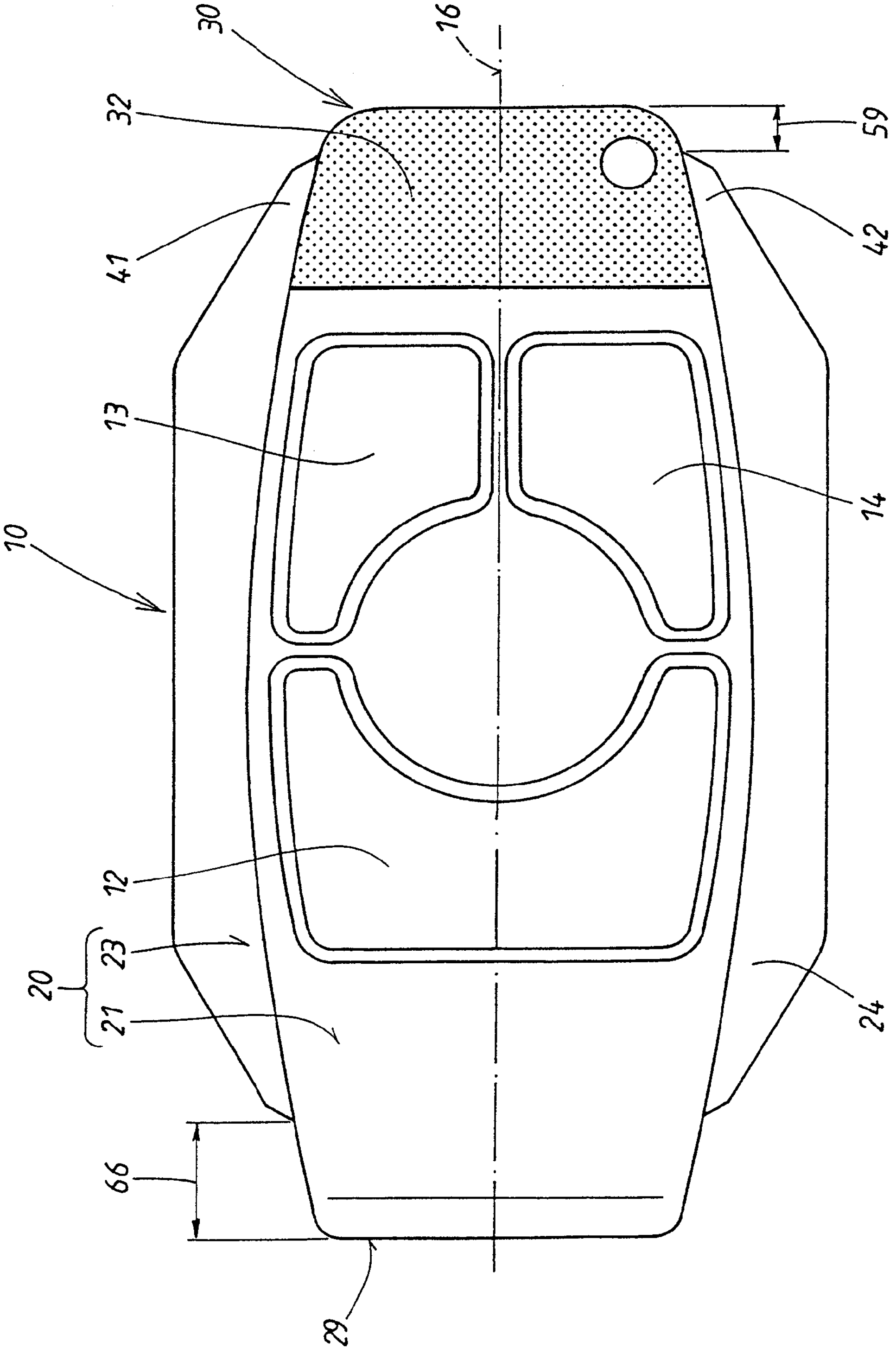


FIG. 1

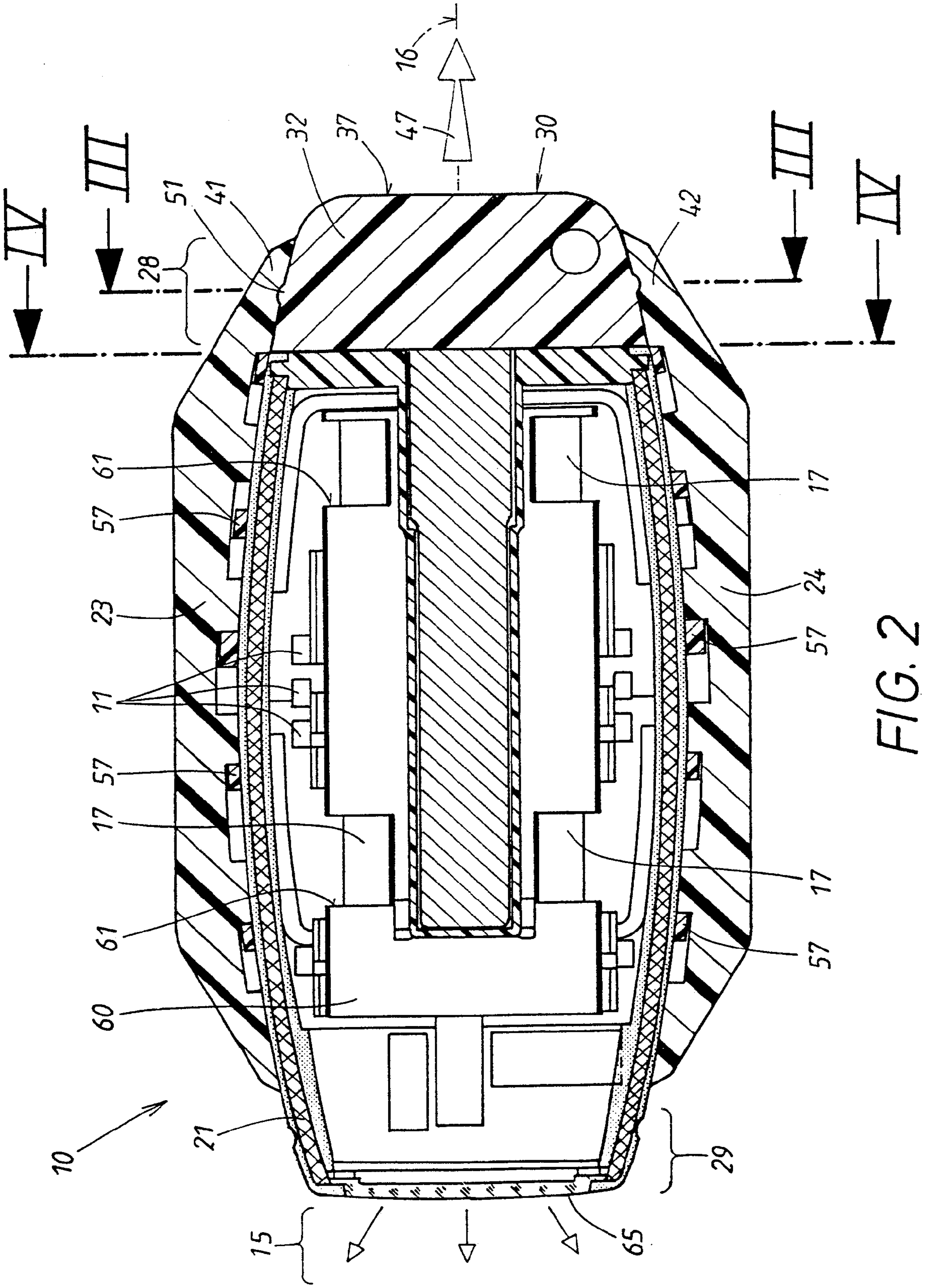

16
47
32
37
30
IV
III
51
41
28
42
III
IV
61
57
23
11
57
17
61
60
10
21
15
65
29
17
24
57
17
57

FIG. 2

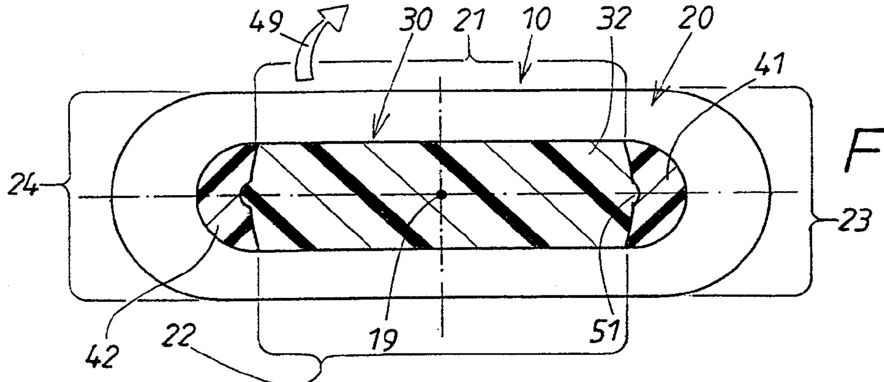


FIG. 3

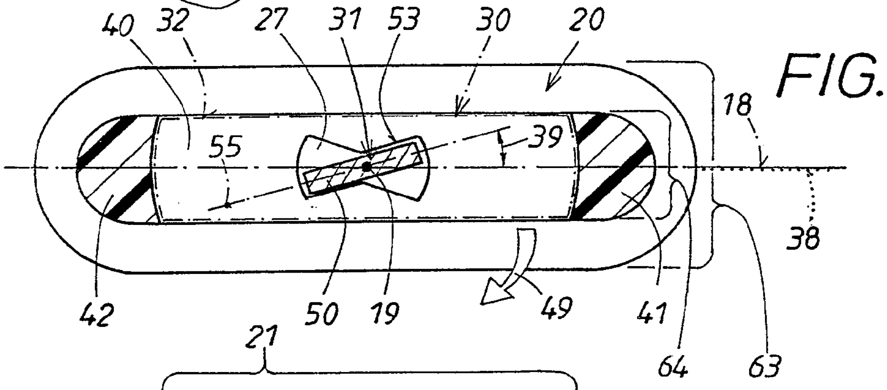


FIG. 4

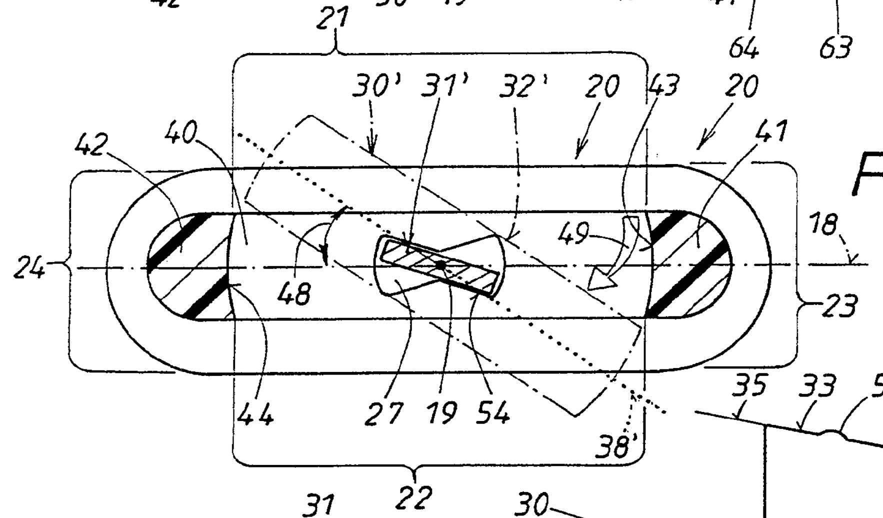


FIG. 5

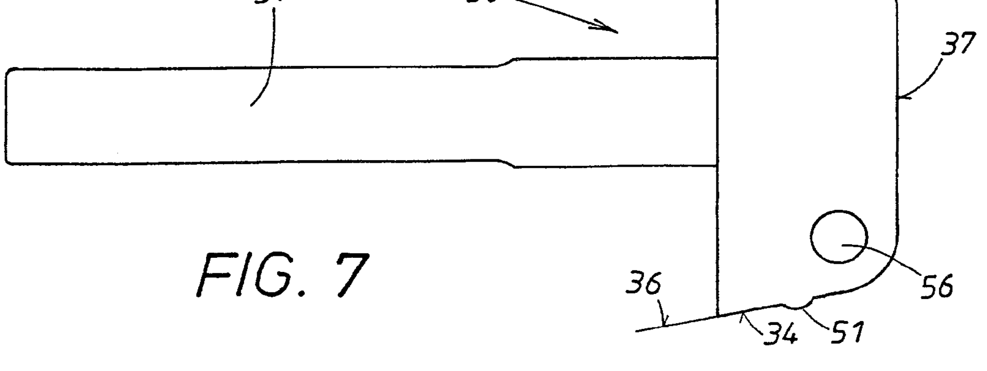


FIG. 7

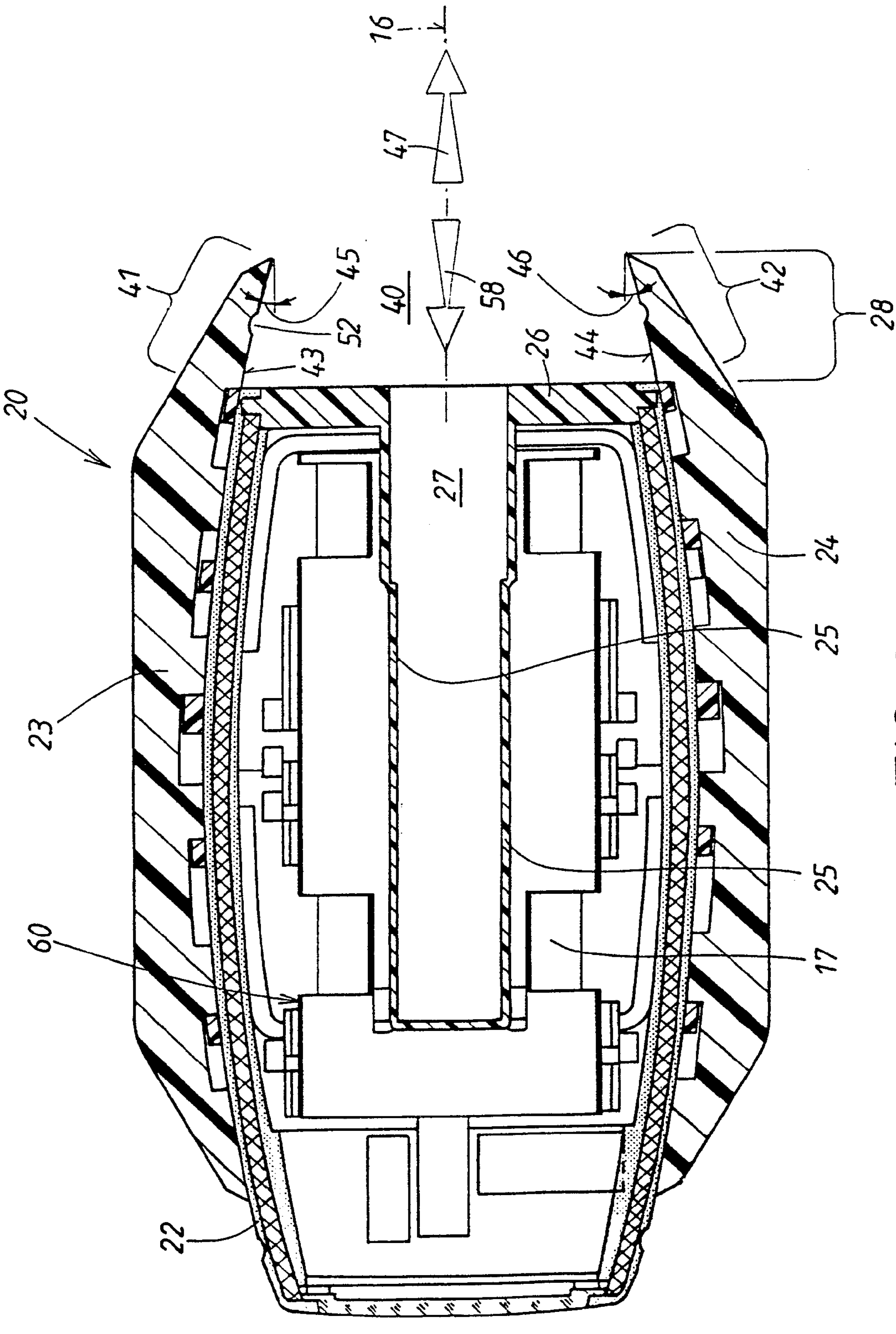


FIG. 6

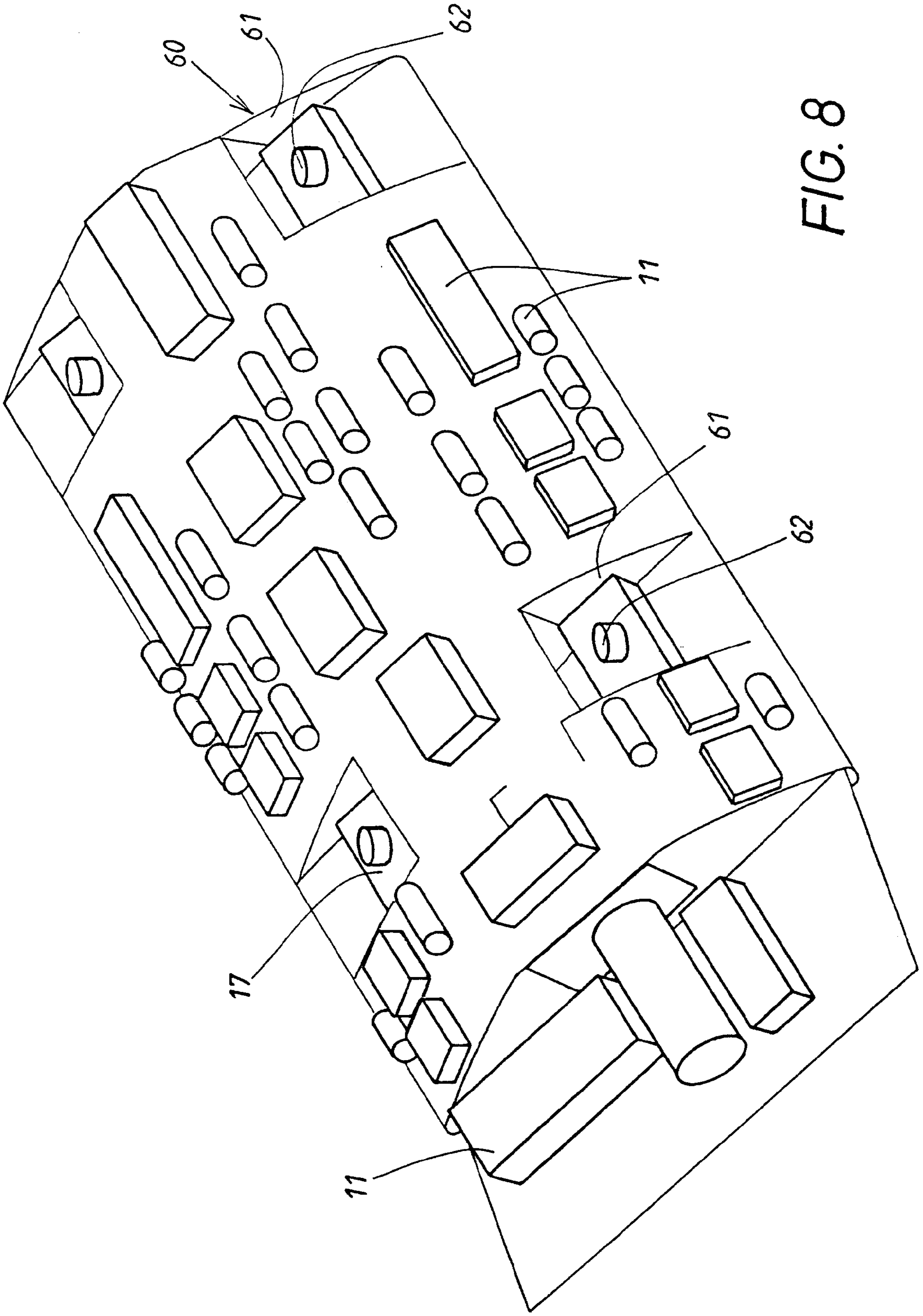


FIG. 8

INTERNATIONAL SEARCH REPORT

Int ional Application No
PCT/EP 99/09251

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 E05B49/00 E05B19/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 7 E05B

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE 297 22 484 U (HUF HUELSBECK & FUERST GMBH &) 26 February 1998 (1998-02-26) figures page 2, last paragraph -page 3, paragraph 1 page 4, paragraph 1 - paragraph 2	1,2
A	DE 44 44 913 A (MARQUARDT GMBH) 22 June 1995 (1995-06-22) abstract; figures 1,3,5,7,8	1,2
A	DE 197 23 039 A (WISUSCHIL ANDREAS) 3 December 1998 (1998-12-03) abstract; figure 3 column 3, line 29 - line 37	1

□ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search 16 February 2000	Date of mailing of the international search report 24/02/2000
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Authorized officer Buron, E

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte onal Application No
PCT/EP 99/09251

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
DE 29722484	U	26-02-1998	NONE	
DE 4444913	A	22-06-1995	NONE	
DE 19723039	A	03-12-1998	NONE	

INTERNATIONALER RECHERCHENBERICHT

Int. ionales Aktenzeichen
PCT/EP 99/09251

A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES
IPK 7 E05B49/00 E05B19/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

B. RECHERCHIERTE GEBIETE

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)
IPK 7 E05B

Recherchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die recherchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	DE 297 22 484 U (HUF HUELSBECK & FUERST GMBH &) 26. Februar 1998 (1998-02-26) Abbildungen Seite 2, letzter Absatz -Seite 3, Absatz 1 Seite 4, Absatz 1 - Absatz 2	1,2
A	DE 44 44 913 A (MARQUARDT GMBH) 22. Juni 1995 (1995-06-22) Zusammenfassung; Abbildungen 1,3,5,7,8	1,2
A	DE 197 23 039 A (WISUSCHIL ANDREAS) 3. Dezember 1998 (1998-12-03) Zusammenfassung; Abbildung 3 Spalte 3, Zeile 29 - Zeile 37	1

☐ Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

☒ Siehe Anhang Patentfamilie

° Besondere Kategorien von angegebenen Veröffentlichungen :

"A" Veröffentlichung, die den allgemeinen Stand der Technik definiert, aber nicht als besonders bedeutsam anzusehen ist

"E" älteres Dokument, das jedoch erst am oder nach dem internationalen Anmeldedatum veröffentlicht worden ist

"L" Veröffentlichung, die geeignet ist, einen Prioritätsanspruch zweifelhaft erscheinen zu lassen, oder durch die das Veröffentlichungsdatum einer anderen im Recherchenbericht genannten Veröffentlichung belegt werden soll oder die aus einem anderen besonderen Grund angegeben ist (wie ausgeführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Benutzung, eine Ausstellung oder andere Maßnahmen bezieht

"P" Veröffentlichung, die vor dem internationalen Anmeldedatum, aber nach dem beanspruchten Prioritätsdatum veröffentlicht worden ist

"T" Spätere Veröffentlichung, die nach dem internationalen Anmeldedatum oder dem Prioritätsdatum veröffentlicht worden ist und mit der Anmeldung nicht kollidiert, sondern nur zum Verständnis des der Erfindung zugrundeliegenden Prinzips oder der ihr zugrundeliegenden Theorie angegeben ist

"X" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann allein aufgrund dieser Veröffentlichung nicht als neu oder auf erfinderischer Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderischer Tätigkeit beruhend betrachtet werden, wenn die Veröffentlichung mit einer oder mehreren anderen Veröffentlichungen dieser Kategorie in Verbindung gebracht wird und diese Verbindung für einen Fachmann naheliegend ist

"&" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche 16. Februar 2000	Absendedatum des internationalen Recherchenberichts 24/02/2000
Name und Postanschrift der Internationalen Recherchenbehörde Europäisches Patentamt, P.B. 5818 Patentlaan 2 NL – 2280 HV Rijswijk Tel. (+31–70) 340–2040, Tx. 31 651 epo nl, Fax: (+31–70) 340–3016	Bevollmächtigter Bediensteter Buron, E

INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Inte   onales Aktenzeichen
PCT/EP 99/09251

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 29722484 U	26-02-1998	KEINE	
DE 4444913 A	22-06-1995	KEINE	
DE 19723039 A	03-12-1998	KEINE	

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : **G06F 1/00**	**A1**	**(11) International Publication Number:** **WO 00/42491** **(43) International Publication Date:** 20 July 2000 (20.07.00)

(21) International Application Number: PCT/US00/00711

(22) International Filing Date: 12 January 2000 (12.01.00)

(30) Priority Data:

60/116,006	15 January 1999 (15.01.99)	US
09/281,017	30 March 1999 (30.03.99)	US
09/449,159	24 November 1999 (24.11.99)	US

(71) Applicant: RAINBOW TECHNOLOGIES, INC. [US/US]; 50 Technology Drive, Irvine, CA 92618 (US).

(72) Inventors: ABBOTT, Shawn, D.; 305 Pinnacle Ridge Place, RR12, Calgary, Alberta T3E 6W3 (CA). AFGHANI, Bahram; 891 Tia Juana Street, Laguna Beach, CA 92651 (US). SOTOODEH, Mehdi; 17 Paloma Drive, Mission Viejo, CA 92692 (US). DENTON, Norman, L., III; 34052 Capo–by–the–Sea, Dana Point, CA 92629 (US). LONG, Calvin, W.; 1260 Oakhaven Lane, Arcadia, CA 91006 (US). PUNT, Maarten, G.; 24942 Paseo Arboleda, Lake Forest, CA 92630 (US). ANDERSON, Allan, D.; 11158 Bertha Place, Cerritos, CA 90703 (US). GODDING, Patrick, N.; 22665 Shady Grove Circle, Lake Forest, CA 92630 (US).

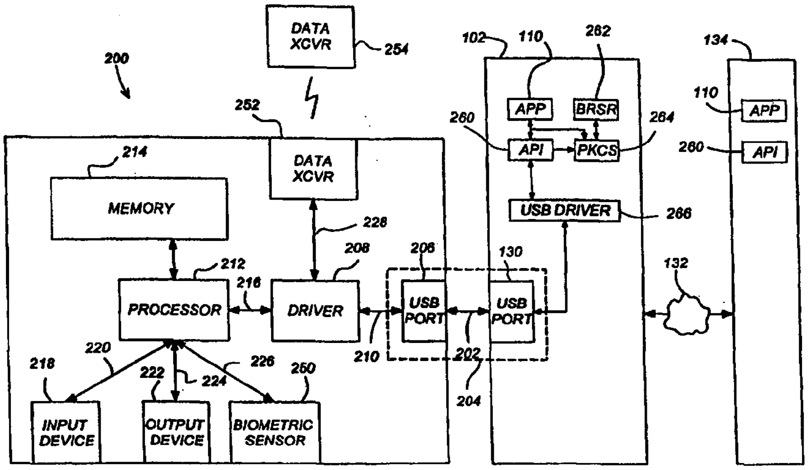
(74) Agent: COOPER, Victor, G.; Gates & Cooper, Suite 1050, 6701 Center Drive, West, Los Angeles, CA 90025 (US).

(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published

With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: USB–COMPLIANT PERSONAL KEY WITH INTEGRAL INPUT AND OUTPUT DEVICES



(57) Abstract

A compact, self–contained, personal key is disclosed. The personal key comprises a USB–compliant interface (206) releasably coupleable to a host processing device (102); a memory (214); and a processor (212). The processor (212) provides the host processing device (102) conditional access to data storable in the memory (214) as well as the functionality required to manage files stored in the personal key and for performing computations based on the data in the files. In one embodiment, the personal key also comprises an integral user input device (218) and an integral user output device (222). The input and output devices (218, 222) communicate with the processor (212) by communication paths (220, 222) which are independent from the USB–compliant interface (206), and thus allow the user to communicate with the processor (212) without manifesting any private information external to the personal key.

FOR THE PURPOSES OF INFORMATION ONLY

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

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

USB-COMPLIANT PERSONAL KEY WITH INTEGRAL INPUT AND OUTPUT DEVICES

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to computer peripherals, and in particular to a personal key having input and output devices integrated therewith to provide for increased security.

2. Description of the Related Art

In the last decade, the use of personal computers in both the home and in the office have become widespread. These computers provide a high level of functionality to many people at a moderate price, substantially surpassing the performance of the large mainframe computers of only a few decades ago. The trend is further evidenced by the increasing popularity of laptop and notebook computers, which provide high-performance computing power on a mobile basis.

The widespread availability of personal computers has had a profound impact on interpersonal communications as well. Only a decade ago, telephones or fax machines offered virtually the only media for rapid business communications. Today, a growing number of businesses and individuals communicate via electronic mail (e-mail). Personal computers have also been instrumental in the emergence of the Internet and its growing use as a medium of commerce.

While certainly beneficial, the growing use of computers in personal communications, commerce, and business has also given rise to a number of unique challenges.

First, the growing use of computers has resulted in extensive unauthorized use and copying of computer software, costing software developers substantial revenue. Although unauthorized copying or use of software is a violation of the law, the widespread availability of pirated software and enforcement difficulties have limited the effectiveness of this means of preventing software piracy.

Software developers and computer designers alike have sought technical solutions to attack the problem of software piracy. One solution uses an external device known as a hardware key, or "dongle" coupled to an input/output (I/O) port of the host computer.

While the use of such hardware keys is an effective way to reduce software piracy, to date, their use has been substantially limited to high value software products. Hardware keys have not been widely applied to popular software packages, in part, because the hardware keys are too expensive, and in part, because there is a reluctance on the part of the application program user to bother with a hardware key whenever use of the protected program is desired. Also, in many cases, the hardware keys are designed for use with only one application. Hence, where the use of multiple applications on the same computer is desired, multiple hardware keys must be operated at the same time.

While it reflects a tremendous advance over telephones and facsimile machines, e-mail also has its problems. One of these problems involves security. Telephone lines are relatively secure and a legally sanctioned way to engage in the private transmission of information, however, e-mails are generally sent over the Internet with no security whatsoever. Persons transmitting electronic messages must be assured that their messages are not opened or disclosed to unauthorized persons.

Further, the addressee of the electronic message should be certain of the identity of the sender and that the message was not tampered with at some point during transmission.

Although the packet-switching nature of Internet communications helps to minimize the risk of intercepted communications, it would not be difficult for a determined interloper to obtain access to an unprotected e-mail message.

Many methods have been developed to secure the integrity of electronic messages during transmission. Simple encryption is the most common method of securing data. Both secret key encryption such as DES (Data Encryption Standard) and public key encryption methods that use both a public and a private key are implemented. Public and private key encryption methods allow users to send Internet and e-mail messages without concern that the message will be read by unauthorized persons or that its contents will be tampered with. However, key cryptographic methods do not protect the receiver of the message, because they do not allow the recipient to authenticate the validity of the public key or to validate the identity of the sender of the electronic message.

The use of digital certificates presents one solution to this problem. A digital certificate is a signed document attesting to the identity and public key of the person signing the message. Digital certificates allow the recipient to validate the authenticity of a public key. However, the typical user may use e-mail to communicate with hundreds of persons, and may use any one of several computers to do so. Hence, a means for managing a number of digital certificates across several computer platforms is needed.

Internet commerce raises other challenges. Users seeking to purchase goods or services using the Internet must be assured that their credit card numbers and the like are safe from compromise. At the same time, vendors must be assured that services and goods are delivered only to those who have paid for them. In many cases, these goals are accomplished with the use of passwords. However, as Internet commerce becomes more commonplace, customers are finding themselves in a position where they must either decide to use a small number of passwords for all transactions, or face the daunting task of remembering multiple passwords. Using a small number of passwords for all transactions inherently compromises security, since the disclosure of any of the passwords may lead to a disclosure of the others. Even the use of a large number of passwords can lead to compromised security. Because customers commonly forget their password, many Internet vendors provide an option whereby the user can be reminded of their password by providing other personal information such as their birthplace, mother's maiden name, and/or social security number. This feature, while often necessary to promote Internet commerce, severely compromises the password by relying on "secret" information that is in fact, publicly available.

Even in cases where the user is willing and able to keep track of a large number of passwords, the password security technique is often compromised by the fact that the user is inclined to select a password that is relatively easy to remember. It is indeed rare that a user selects a truly random password. What is needed is a means for generating and managing random passwords that can be stored and recalled for use on a wide variety of computer platforms.

Internet communications have also seen the increased use of "cookies." Cookies comprise data and programs that keep track of a user's patterns and preferences that can be downloaded from the Internet server for storage on the user's computer. Typically, cookies contain a range of addresses. When the browser encounters those addresses again, the cookies associated with the addresses are provided to the Internet server. For example, if a user's password were stored as a cookie, the use of the cookie would allow the user to request services or goods without requiring that the user enter the password again when accessing that service for the second and subsequent time.

However beneficial, cookies can also have their dark side. Many users object to storage of cookies on their computer's hard drive. In response to these concerns, Internet browser software allows the user to select an option so that they are notified before cookies are stored or used. The trouble with this solution is that this usually results in an excessive number of messages prompting the user to accept cookies. A better solution than this all-or-nothing approach would be to allow the storage and/or use of cookies, but to isolate and control that storage and use to comply with user-specified criteria.

Smartcard provide some of the above mentioned functionality, but smartcards do not present an ideal solution. First, personal keys are only valuable to the user if they offer a single, widely accepted secure repository for digital certificates and passwords. Smartcard readers are relatively expensive, and are not in wide use, at least in the United States, and are therefore unsuited to the task.

Second, smartcards do not provide for entering data directly into the card. This opens the smartcard to possible sniffer modules in malicious software, which can monitor the smartcard-reader interface to determine the user's personal identification or password information. This problem is especially problematic in situations where the user is using an unknown or untrusted smartcard reader. The lack of any direct input device also prevents the user from performing any smartcard-related functions in the relatively common situation where no smartcard reader is available.

Third, data cannot be accessed from the smartcard unless the smartcard is in the reader. This prevents the user from viewing data stored in the smartcard (i.e. a stored password) until a smartcard reader can be located. Given that smartcard readers (especially trusted ones) can be difficult to find, this substantially limits the usefulness of the card. Of course, the user may simply write the password down on paper, but this may compromise the security of all of the data in the card, and is inconsistent with the goal of providing a central, secure, portable repository for private data.

From the foregoing, it can be seen that there is a need for a personal key that allows the user to store and retrieve passwords and digital certificates without requiring the use of vulnerable external interfaces.

SUMMARY OF THE INVENTION

The present invention satisfies all of these needs with a personal key in a form factor that is compliant with a commonly available I/O interface such as the Universal Serial Bus (USB). The personal key includes a processor and a memory which implement software protection schemes to prevent copying and unauthorized use.

The personal key provides for the storage and management of digital certificates, allowing the user to store all of his digital certificates in one media that is portable from platform to platform. The personal key provides for the generation, storage, and management of many passwords, providing additional security and relieving the user from the task of remembering multiple passwords. The personal key provides a means to store cookies and other Java-implemented software programs, allowing the user to accept cookies in a removable and secure form-factor. These features are especially useful when the present invention is used in a virtual private network (VPN). The present invention can also be used for several applications

Because the personal key is capable of storing virtually all of the user's sensitive information, it is important that the personal key be as secure as possible. Hence, one embodiment of the personal key also comprises a biometric sensor disposed to measure biometrics such as fingerprint data. The biometric sensor measures characteristics of the person holding the key (such as fingerprints) to confirm that the person possessing the key is the actual owner of the key.

Since the personal key represents a single, secure repository for a great deal of the data the user will need to use and interact with a variety of computer platforms, it is also important that the personal key be able to interface (i.e., transmit and receive data) with a large variety of computers and computer peripherals. Hence, one embodiment of the personal key includes an electromagnetic wave transception device such as an infrared (IR) transceiver. This transceiver allows the personal key to exchange information with a wide variety of computers and peripherals without physical coupling.

The present invention is well suited for controlling access to network services, or anywhere a password, cookie, digital certificate, or smartcard might otherwise be used, including:

- Remote access servers, including Internet protocol security (IPSec), point to point tunneling protocol (PPTP), password authentication protocol (PAP), challenge handshake authentication protocol (CHAP), remote access dial-in user service (RADIUS), terminal access controller access control system (TACACS);

- Providing Extranet and subscription-based web access control, including hypertext transport protocol (HTTP), secure sockets layer (SSL);
- Supporting secure online banking, benefits administration, account management;
- Supporting secure workflow and supply chain integration (form signing);
- Preventing laptop computer theft (requiring personal key for laptop operation);
- Workstation logon authorization;
- Preventing the modification or copying of software;
- Encrypting files;
- Supporting secure e-mail, for example, with secure multipurpose Internet mail extensions (S/MIME), and open pretty good privacy (OpenPGP)
- Administering network equipment administration; and
- Electronic wallets, with, for example, secure electronic transaction (SET, MilliCent, eWallet)

In one embodiment, the present invention comprises a compact, self-contained, personal token or key. The personal key comprises a USB-compliant interface releaseably coupleable to a host processing device; a memory; and a processor. The processor provides the host processing device conditional access to data storable in the memory as well as the functionality required to manage files stored in the personal key and for performing computations based on the data in the files. In one embodiment, the personal key also comprises an integral user input device and an integral user output device. The input and output devices communicate with the processor by communication paths which are independent from the USB-compliant interface, and thus allow the user to communicate with the processor without manifesting any private information external to the personal key.

BRIEF DESCRIPTION OF THE DRAWINGS

Referring now to the drawings in which like reference numbers represent corresponding parts throughout:

FIG. 1 is a diagram showing an exemplary hardware environment for practicing the present invention;

FIG. 2 is a block diagram illustrating selected modules of one embodiment of the present invention;

FIG. 3 is a diagram of the memory resources provided by the memory of the personal key;

FIG. 4 is a diagram showing one embodiment of how an encryption engine is used to authenticate the identity of the personal key or the application data stored therein;

FIG. 5 is a diagram illustrating the data contents of a file system memory resource of an active personal key that provides authentication and specific configuration data for several application;

FIG. 6 is a diagram presenting an illustration of one embodiment of the personal key;

FIGs. 7A-7C are diagrams showing one embodiment of the personal key having an input device including a first pressure sensitive device and a second pressure sensitive device, each communicatively coupled the processor by a communication path distinct from the USB-compliant interface;

FIGs. 8A-8C are diagrams presenting an illustration of another embodiment of the present invention;

FIG. 9 is a flow chart illustrating an embodiment of the present invention in which processor operations are subject to user authorization; and

FIG. 10 is a flow chart illustrating an embodiment of the present invention in which the PIN is entered directly into the personal key.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

In the following description, reference is made to the accompanying drawings which form a part hereof, and which is shown, by way of illustration, several embodiments of the present invention. It is understood that other embodiments may be utilized and structural changes may be made without departing from the scope of the present invention.

Hardware Environment

FIG. 1 illustrates an exemplary computer system 100 that could be used to implement the present invention. The computer 102 comprises a processor 104 and a memory, such as random access memory (RAM) 106. The computer 102 is operatively coupled to a display 122, which presents images such as windows to the user on a graphical user interface 118B. The computer 102 may be coupled to other devices, such as a keyboard 114, a mouse device 116, a printer 128, etc. Of course, those skilled in the art will recognize that any combination of the above components, or any number of different components, peripherals, and other devices, may be used with the computer 102.

Generally, the computer 102 operates under control of an operating system 108 stored in the memory 106, and interfaces with the user to accept inputs and commands and to present results through a graphical user interface (GUI) module 118A. Although the GUI module 118A is depicted as a separate module, the instructions performing the GUI functions can be resident or distributed in the operating system 108, the computer program 110, or implemented with special purpose memory and processors. The computer 102 also implements a compiler 112 which allows an application program 110 written in a programming language such as COBOL, C++, FORTRAN, or other language to be translated into processor 104 readable code. After completion, the application 110 accesses and manipulates data stored in the memory 106 of the computer 102 using the relationships and logic that are generated using the compiler 112. The computer 102 also comprises an input/output (I/O) port 130 for a personal token 200 (hereinafter alternatively referred to also as a personal key 200). In one embodiment, the I/O port 130 is a USB-compliant port implementing a USB-compliant interface.

In one embodiment, instructions implementing the operating system 108, the computer program 110, and the compiler 112 are tangibly embodied in a computer-readable medium, e.g., data storage device 120, which could include one or more fixed or removable data storage devices, such as a zip drive, floppy disc drive 124, hard drive, CD-ROM drive, tape drive, etc. Further, the operating system 108 and the computer program 110 are comprised of instructions which, when read and executed by the computer 102, causes the computer 102 to perform the steps necessary to implement and/or use the present invention. Computer program 110 and/or operating instructions may also be tangibly embodied in memory 106 and/or data communications devices, thereby making a computer program product or article of manufacture according to the invention. As such, the terms "article of manufacture" and "computer program product" as used herein are intended to encompass a computer program accessible from any computer readable device or media.

The computer 102 may be communicatively coupled to a remote computer or server 134 via communication medium 132 such as a dial-up network, a wide area network (WAN), local area network (LAN), virtual private network (VPN) or the Internet. Program instructions for computer operation, including additional or alternative application programs can be loaded from the remote computer/server 134. In one embodiment, the computer 102 implements an Internet browser, allowing the user to access the world wide web (WWW) and other internet resources.

Those skilled in the art will recognize that many modifications may be made to this configuration without departing from the scope of the present invention. For example, those skilled in the art will recognize that any combination of the above components, or any number of different components, peripherals, and other devices, may be used with the present invention.

Architectural Overview

FIG. 2 is a block diagram illustrating selected modules of the present invention. The personal key 200 communicates with and obtains power from the host computer through a USB-compliant communication path 202 in the USB-compliant interface 204 which includes the input/output port 130 of the host computer 102 and a matching input/output (I/O) port 206 on the personal key 200. Signals received at the personal key I/O port 206 are passed to and from the processor 212 by a driver/buffer 208 via communication paths 210 and 216. The processor 212 is communicatively coupled to a memory 214, which may store data and instructions to implement the above-described features of the invention. In one embodiment, the memory 214 is a non-volatile random-access memory that can retain factory-supplied data as well as customer-supplied application related data. The processor 212 may also include some internal memory for performing some of these functions.

The processor 212 is optionally communicatively coupled to an input device 218 via an input device communication path 220 and to an output device 222 via an output device communication path 224, both of which are distinct from the USB-compliant interface 204 and communication path 202. These separate communication paths 220 and 224 allow the user to view information about processor 212 operations and provide input related to processor 212 operations without allowing a process or other entity with visibility to the USB-compliant interface 204 to eavesdrop or intercede. This permits secure communications between the key processor 212 and the user. In one embodiment of the invention set forth more fully below, the user communicates directly with the processor 212 by physical manipulation of mechanical switches or devices actuatable from the external side of the key (for example, by pressure-sensitive devices such as buttons and mechanical switches). In another embodiment of the invention set forth more fully below, the input device includes a wheel with tactile detents indicating the selection of characters.

The input device and output devices 218, 222 may cooperatively interact with one another to enhance the functionality of the personal key 200. For example, the output device 222 may provide information prompting the user to enter information into the input device 218. For example, the output device 222 may comprise a visual display such as an alphanumeric LED or LCD display (which can display Arabic numbers and or letters) and/or an aural device. The user may be prompted to enter information by a beeping of the aural device, by a flashing pattern of the LED, or by both. The output device 222 may also optionally be used to confirm entry of information by the input device 218. For example, an aural output device may beep when the user enters information into the input device 218 or when the user input is invalid. The input device 218 may take one of many forms, including different combinations of input devices.

Although the input device communication path 220 and the output device communication path 224 are illustrated in FIG. 2 as separate paths, the present invention can be implemented by combining the paths 220 and 224 while still retaining a communication path distinct from the USB-compliant interface 204. For example, the input device 218 and output device 222 may be packaged in a single device and communications with the processor 212 multiplexed over a single communication path.

In one embodiment of the invention, the present invention further comprises a second output device 222 that may be coupled to the USB-compliant interface 204 instead of being coupled to the processor via a communication path distinct from the USB-compliant interface 204. This embodiment may be used, for example, to indicate to the user that the personal key 200 has been correctly inserted into the host computer's USB port (for example, by providing an indication of a power signal of the USB-compliant interface). The second output device may also be used to show that data is passing to and from the host computer and the personal key 200 (for example, by providing an indication of a data signal from the USB-compliant interface).

The personal key has an interface including a USB driver module 266 communicatively coupled to an application program interface (API) 260 having a plurality of API library routines. The API 260 provides an interface with the application 110 to issue commands and accept results from the personal key 200. In one embodiment, a browser 262, such as the browser available from NETSCAPE, Inc. operates with the API 260 and the public key cryptographic standard (PKCS) module 264 to implement a token-based user authentication system.

While the portability and utility of the personal key has many advantages, it also has one important disadvantage...it can be lost or stolen. This is especially troublesome because the personal key 200 represents a secure repository for so much of the user's private data. For these reasons, the ultimate security of the information contained in the personal key 200 (but not necessarily the personal key 200 itself) is highly important.

Ultimately, the personal key 200 identifies the possessor to the outside world through the host computer 102, but there is no guarantee that the person in possession of the personal key 200 is the actual owner, because the personal key may have been lost or stolen. Security can be increased with the use of personal passwords and the like, but this solution is not ideal. First, the use of a single password raises the very real possibility that the password may have been compromised (after all, the thief may know the user, and hence, the user's password). Also, requiring the entry of a password multiple times increases the chance that malicious software executing in the host computer 102 or the remote computer 134 may eavesdrop on the password or personal identification. The use of multiple passwords is no solution because one of the reasons for using the personal key 200 is to relieve the user of the need to remember a number of passwords. Another problem with passwords is that hacking methods can be employed to circumvent the password protection or to discover the password itself. This is especially problematic in context of a personal key 200 which in most cases, depends on data entered in a host computer 120 peripheral such as the keyboard 114 and transmitted via the input/output port 130, rendering the personal key 200 vulnerable to hacking.

In one embodiment of the present invention, a biometric sensing device 250 is mounted on or in the personal key 200 to collect biometric data from the user when the user is holding the personal key 200. In one embodiment, the biometric sensing device 250 comprises a fingerprint sensor, which is capable of reading the user's fingerprints. The biometric sensor 250 may also include built-in processing to reduce the biometric data to data suitable for use by the processor 212. If necessary for the collection of biometric data, a light emitting or heat-emitting device can be placed proximate to the biometric sensor to provide an active data measurement using light or heat.

The biometric sensor 250 is nominally placed where it can best measure the biometric data of interest. In the illustrated embodiment, the biometric sensor 250 is sized and disposed to collect data from the user's thumbprint when the user grips the personal key 200 to insert it into the host computer 102 I/O port 130. To facilitate measurement of the holder's fingerprint, the exterior surface of the personal key 200 can be designed to cradle the user's thumb in a particular place. Alternatively, to increase security, the exterior appearance of the personal key 200 may be designed to mask the presence of the biometric sensor 250 entirely.

The biometric sensor 250 can be advantageously placed in a position where it can be expected to collect known data of a predictable type, at a known time (for example, obtaining a thumbprint when the personal key 200 is plugged into the host computer I/O port 130). The personal key 200 accepts data from the biometric sensor 250 via biometric sensor communication path 226 to verify the identity of the person holding the key with no passwords to remember or compromise, or any other input. Thus, the biometric sensor 250 provides a personal key 200 with a heightened level of security which is greater than that which can be obtained with a biometric sensor or passwords alone. If necessary, the personal key 200 can be configured to recognize the host computer 102 it is plugged into, and using data thus obtained, further increase the security of the key.

The biometric sensor can also be used to increase the security of the personal key in other ways as well. For example, if the personal key were to be stolen, the biometric sensor can be used to measure the fingerprint of the thief. This data can be stored and retained until such time as the thief attempts to use the personal key to make a purchase, for example on the Internet. At this time, the personal key 200 can be programmed to contact (with or without visibility to the thief) a particular entity (such as an Internet site), where the fingerprint information (and any other relevant information) can be transferred to the appropriate authority. The personal key 200 may also perform this dial up and report function if a number of incorrect passwords have been supplied.

In one embodiment of the present invention, the personal key 200 also comprises a data transceiver 252 for communicating data with an external data transceiver 254. The data transceiver 252 is communicatively coupled to the processor 212, via the driver 208 and communication paths 216 and 228, and allows the personal key 200 to transmit and receive data via the transmission and reception of electromagnetic waves without exposing the data to the USB-compliant interface 204. Alternatively, the data transceiver 252 may be communicatively coupled directly to the processor 212.

In one embodiment, the data transceiver 252 comprises an infrared (IR) transceiver that can communicate with a number of commercially available peripherals with similar capability. This feature provides the personal key 200 another means for communicating with external peripherals and devices, even when the personal key 200 is already coupled to the I/O port 130 of the host computer 102.

In one embodiment, the personal key 200 also comprises a power source such as a battery or capacitive device. The power source supplies power to the components of the personal key to allow the data to be retained and to allow personal key functions and operations to be performed, even when disconnected from the host computer 102.

FIG. 3 is a diagram of the memory resources provided by the memory 214 of the personal key 200. The memory resources include a master key memory resource 312, a personal identification number (PIN) memory resource 314, an associated PIN counter register 316 and PIN reset register resource 318, a serial number memory resource 310, a global access control register memory resource 320, a file system space 324, auxiliary program instruction space 322, and a processor operation program instruction space 326. The processor operation program instruction space 326 stores instructions that the personal key 200 executes to perform the nominal operations described herein, including those supporting functions called by the application program interface 260 associated with the applications 110 executing in either the host computer 102 or the remote server 134. The auxiliary program instruction space provides the personal key 200 with space to store processor 212 instructions for implementing additional functionality, if desired.

The master key is an administrative password that must be known by the trusted entity or program that will initialize and configure the personal key 200. For example, if the personal key 200 is to be supplied to a number of remotely located employees to enable access to private documents stored in a remote server through a VPN, the system administrator for the remote server may enter the master key (or change the key from the factory settings) before providing the key to the remotely located employees. The system administrator also stores the master key in a secure place, and uses this master key to perform the required secure operations (including, for example, authorization and authentication of the remote users).

In one embodiment, the master key can not be configured, reset, or initialized if the MKEY can not be verified first. Hence, if the master key is unknown the personal key 200 would have to be destroyed/thrown away or returned to the factory to be reset to the factory settings.

The PIN is an optional value that can be used to authenticate the user of the personal key 200. The PIN is initialized by the trusted administrator. Depending on how the personal key 200 initialization program is implemented and deployed, it is possible for the end user to set and/or update their PIN. The PIN may comprise alphanumeric characters or simply numbers.

The PIN can also be checked using an application program interface (API) call that transparently uses the two associated registers 316 and 318. The PIN counter resource 316 is a decrementing counter, while the PIN reset register resource 318 is used to store a limit that is used to reset the PIN counter 316 memory resource. The PIN count and limit registers 316 and 318 are used to prevent a rogue application or user from rapidly testing thousands of random PINs in an attempt to discover the PIN.

When the PIN is initialized, the decrementing counter register 316 is set to the value in the PIN reset register resource 318. Whenever a PIN verification fails the counter register 316 is decremented. When a PIN verification succeeds then the counter register is set to the limit value. When the decrementing counter register 316 reaches 0, no more PIN verifications are permitted until a trusted administrator resets the PIN counter register 316 to the limit value. For example if the PIN reset register resource 318 limit has been set to 3, then a user could fail PIN verification 3 times whereupon the PIN would be rendered useless until it is reset. The counter register 316 would be reset to 3 when a correct PIN was successfully verified.

The serial number is a unique factory installed serial number (SN). The serial number can be used to differentiate a single user from all other personal key 200 users.

The memory 214 of the personal key 200 also includes built in algorithm memory resources 302, including a MD-5 hash engine memory 304 for storing related processing instructions, an HMAC-MD5 authorization memory resource 306 for storing related processing instructions, and a random number generator memory resource 308 for storing processing instructions for generating random numbers. The random number generator can be used to generate challenges to be used when generating authentication digest results as well as to provide seeds to other cryptographic procedures. The MD-5 algorithm accepts as an input a message of arbitrary length, and produces a 128-bit "fingerprint" or "message digest" of the input as an output. In doing so, the algorithm scrambles or hashes the input data into a reproducible product using a high speed algorithm such as RFC-1321. The hashed message authentication codes (HMAC) can be used in combination with any iterated cryptographic hash function (e.g. MD-5) along with a secret key, to authenticate a message or collection of data. The personal key 200 integrates this method to provide a way for the end user or application data to be authenticated without exposing the secret key.

The present invention allows end user authorization using two security mechanisms. The first mechanism, which is discussed below, allows software running on the host computer 102 or the remote computer/server 134 to authenticate the personal key 200. This first mechanism uses a hashing algorithm and a mutually agreed upon secret value known to both the personal key 200 and the entity attempting to authenticate the personal key. The second mechanism, which is discussed later in this disclosure, allows the personal key 200 to authenticate the user who is trying to use the personal key 200. This second mechanism uses a personal identification number (PIN) to help prevent unauthorized use or access in situations where the key has been lost or stolen. As set forth more fully below, the PIN can be entered directly in the personal key 200, thus increasing security by assuring that the PIN is never exposed external to the personal key 200.

FIG. 4 is a diagram showing one embodiment of how the HMAC-MD5 engine is used to authenticate the identity of the personal key 200 or the application data stored therein. Associated with the personal key 200 and executing either in the host computer 102 or the remote computer/server 134 is a personal key library of functions which are linked with an application executing in the host computer (e.g. application program 110) or in the remote computer/server 134. A hash algorithm 410 is implemented in both the application 110 and the personal key 200. Both the application 110 and the personal key 200 have access to a secret 406. The secret 406B is retained within the memory 214 of the personal key 200 in a location where it cannot be accessed without suitable permission. Typically, secret 406B is stored in the personal key 200 by the system administrator or some other trusted source. Hence, if the user of the personal key 200 is the entity that the application 110 thinks it is, the application's secret 406A and the personal key's secret 406B are the same. This can be verified by a hashing algorithm without exposing the secret. Similarly, if the user of the personal key 200 is not the entity that the application expects, secrets 406A and 406B will be different. This too can be verified by a hashing algorithm without exposing the secret.

A challenge is generated by the application 110, and provided to the hash algorithms 410 accessible to the application 110 and the hash algorithm implemented in the personal key 200. Each hash algorithm applies the challenge and the resident secret to generate a hashed output 412. If the hash algorithms were equivalent and each of the secrets 406A and 406B were the same, the resulting hashed output 412 or digest string in each case should be the same. If the digest strings 412A and 412B compare equal using logic 414 in the application, the personal key 200 is trusted.

Further, if the user authentication was verified, the user is trusted as well. One advantage in this authentication system is that the challenge 408 can be transmitted over untrusted media such as the Internet. The secret 406 remains coded in the application 110 or remote server 134 program and in the personal key 200 where it remains without being exposed to network sniffers/snoopers or potentially compromised user interfaces.

The file system memory resource 324 is fully managed within the application program interface library 260 in either the host computer 102 or the remote server 134. It provides a flexible system for storing, protecting, and retrieving personal key 200 data.

FIG. 5 is a diagram illustrating the data contents of a file system memory resource 324 of an active personal key 200 that provides authentication and specific configuration data for several applications. The master file (MF) 502 is the root directory and uses an identification (ID) of zero (0). The MF 502 may contain pointers 504A and 504B or other designations to data files 506A and 506B, as well as pointers 508A and 508B to directories 510 and 516. Directories and files are defined by an identification (1 ➔ 0xFFFFFFFF for the directories, and 0 ➔ 0xFFFFFFFF for files). The directories 510 and 516 also contain pointers (512A-512B and 518A-518B, respectively) to data files (514A-514B and 520A-520C, respectively).

Three file types are implemented, as shown in Table 1 below:

Type	Access
DATA	Any variable length string of unsigned characters
KEY	Strings that are used as input to cryptographic operations
CTR	Data files that have a decrementing counter (e.g. a counter of 16 bits). The counters range from 0 to XFF and are used to limit the number of times a data file can be read.

Table 1

These file types can be controlled on a per-file basis, according to Table 2 below:

Access Types	File Types		
	DATA	KEY	CTR
Read	Control	Never - no control	Control
Write	Control	Control	Control
Crypt	Always - no control	Control	Always - no control

Table 2

The read and write access type controls govern the transfer of files in the personal key 200 to and from the application 110. The crypt access type is used with KEY file types for performing cryptographic operations including the computation of hash values, encrypting, or decrypting data. When set, the controls defined in Table 2 can have one of four attributes listed in Table 3 below:

Attribute	Access
ALWAYS	Always granted, regardless of whether the proper PIN or MKEY has been supplied to the personal key 200.
NEVER	Never granted, regardless of whether the proper PIN or MKEY has been supplied to the personal key 200.
PIN	Access is granted if and only if the proper PIN has been supplied to the personal key 200, and PIN verification is successful (user authentication).
MKEY	Access is granted if and only if the proper master key (MKEY) has been provided to the personal key 200, and master key verification is successful (super user or security officer authentication).

Table 3

A global access control register 320 applies to the entire scope of the personal key 200 file system. Nominally, the global access control register 320 is an 8-bit value that is divided into two global access controls as shown in Table 4 below:

Global Access Type	Global File System Access
Create	Control
Delete	Control

Table 4

The create and delete global access types can have one of the four attribute values shown in Table 5 below. The create and delete global controls are enforced by the CreateDir, CreateFile, DeleteDir, DeleteFile, and DeleteAllFiles API calls described in Table 5 below.

Attribute	Access
ALWAYS	Always granted, regardless of whether the proper PIN or MKEY has been supplied to the personal key 200.
NEVER	Never granted, regardless of whether the proper PIN or MKEY has been supplied to the personal key 200.
PIN	Access is granted if and only if the proper PIN has been supplied to the personal key 200, and PIN verification is successful (user authentication).
MKEY	Access is granted if and only if the proper MKEY has been supplied to the personal key 200, and PIN verification is successful (super user or security officer authentication).

Table 5

Table 6 is an alphabetical listing of personal key 200 APIs 260 in the library. In Table 6, "D" indicates a device-related function, "F" denotes a file system related function, "A" denotes an administrative function, and "C" denotes a cryptographic function.

Name	Description	D	F	A	C
CloseDevice	Close access to the personal key	√			
CloseFile	Close selected file		√		
CreateDir	Create a directory in the personal key memory		√	√	
CreateFile	Create a file in the personal key memory		√	√	
Decrement	Decrement a CTR type file		√		
DeleteAllFiles	Reformat file space		√	√	
DeleteDir	Delete directory		√	√	
DeleteFile	Delete file		√	√	
Dir	Return directory and file information		√		
GetAccessSettings	Return current global create/delete			√	
GetChallenge	Returns a 64-bit random number			√	√
GetSerialNumber	Read unique serial number	√		√	
HashToken	MD5 hash the selected file or currently open file - two modes are supported (1) XOR hash and HMAC hash		√		√
HMAC_MD5	This function is a wrapper for performing HMAC-MD5 using the HashToken function in the HMAC mode. It computes MD5 without exposing the key.		√		√

Name	Description	D	F	A	C
LedControl	Control the output device, including turning an LED or other output device on or off	√			
ModifyMasterKey	Update/Modify master key			√	
ModifyPIN	Update/Modify PIN			√	
OpenDevice	Open one of 32 potential personal keys	√			
ReadFile	Return contents of selected file		√		
ResetDevice	Reset to power-on state	√		√	
SelectFile	Open a file		√		
SetAccessSettings	Update global create/delete access settings			√	
VerifyMasterKey	Verify the master key provided as an argument is the master key stored in the personal key			√	
VerifyPIN	Verify that the PIN provided as an argument is the PIN stored in the personal key (user authentication)			√	
VerifyPIN2	An alternative command used to verify the user PIN without exposing the PIN externally to the personal key 200. This command is issued without the PIN as an argument, and the personal key 200 returns a response indicating whether the PIN entered by the user on the				√

Name	Description	D	F	A	C
	input device 218 matches that of the stored PIN in the memory 214.				
WriteFile	Write contents to the selected file	√			
MD5_Hash	Hash routine: wrapper (provided in API library and not implemented in personal key)				√
MD5Final	Finish computation and return digest (provided in API library and not implemented in personal key)				√
MD5Init	Initialize message digest context (provided in API library and not implemented in personal key)				√
MD5Update	Update message digest context (provided in API library and not implemented in personal key)				√

Table 6

Exemplary Application to a Virtual Private Network

Using the foregoing, the personal key 200 and related APIs 260 can be used to implement a secure document access system. This secure document access system provides remote users access to secret encrypted documents over the Internet to company employces. The system also limits the circulation of secret encrypted documents so that specified documents can be read only a limited number of times.

The application program 110 used for reading documents is linked with the personal key API 260 library to allow document viewing based on the information in the personal key 200. A trusted administrative program controlled by the master key can be used to set up the personal key 200 (by storing the appropriate information with the associated security control settings) for a wide range of employees.

The personal key 200 and the API 260 library can be used to authenticate document viewers and administrators, to supply keys for decryption and encryption of documents, to provide a list of viewable documents, and to enforce document access rights and counters.

The foregoing can be implemented in a number of programs, including an administrative initialization program to set up the personal keys 200 before delivery to the employees (hereinafter referred to as SETKEY), a document encryption and library update program (hereinafter referred to as BUILDDOC), a viewer application that authenticates the user and the personal key 200 (hereinafter referred to as VIEWDOC), and a library application which authenticates the user and updates the personal key (hereinafter referred to as LIBDOC).

The SETKEY program is used to setup personal keys received from the factory for individual users. Document names, access counters, a PIN, and a hash secret are loaded into the personal key 200. Depending on the employee's security clearance, specific documents can be configured for viewing. For sake of clarification the following symbolic names are used in the discussion below:

DOCFilename -iKey data file that holds the document file name

DOCSecret -iKey data file that holds a secret used to make encryption/decryption keys

First, the SETKEY program gains access to the personal key 200 by issuing an OpenDevice command. The VerifyMasterKey command is then issued to open the personal key 200 to master access. A Dir command is used in a loop to obtain and verify the status of the personal key 200. The comments are compared to the contents of a factory-fresh key, and one of several states is determined. If the key is factory fresh, the personal key is initialized. A VIEWDOC directory and file set is then created. An employee database can then be accessed and used to determine the type and extent of the access that is to be granted to each employee. Depending on the security clearance of each employee, one of several types of directory and file sets can