



01919 U.S. PTO

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

16834 U.S. PTO  
10/990296  
111604

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](http://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 LAN. 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, WI.AN. 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 so 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 appliance. 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 802.11, 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 be 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 cinemplex, 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 an 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.

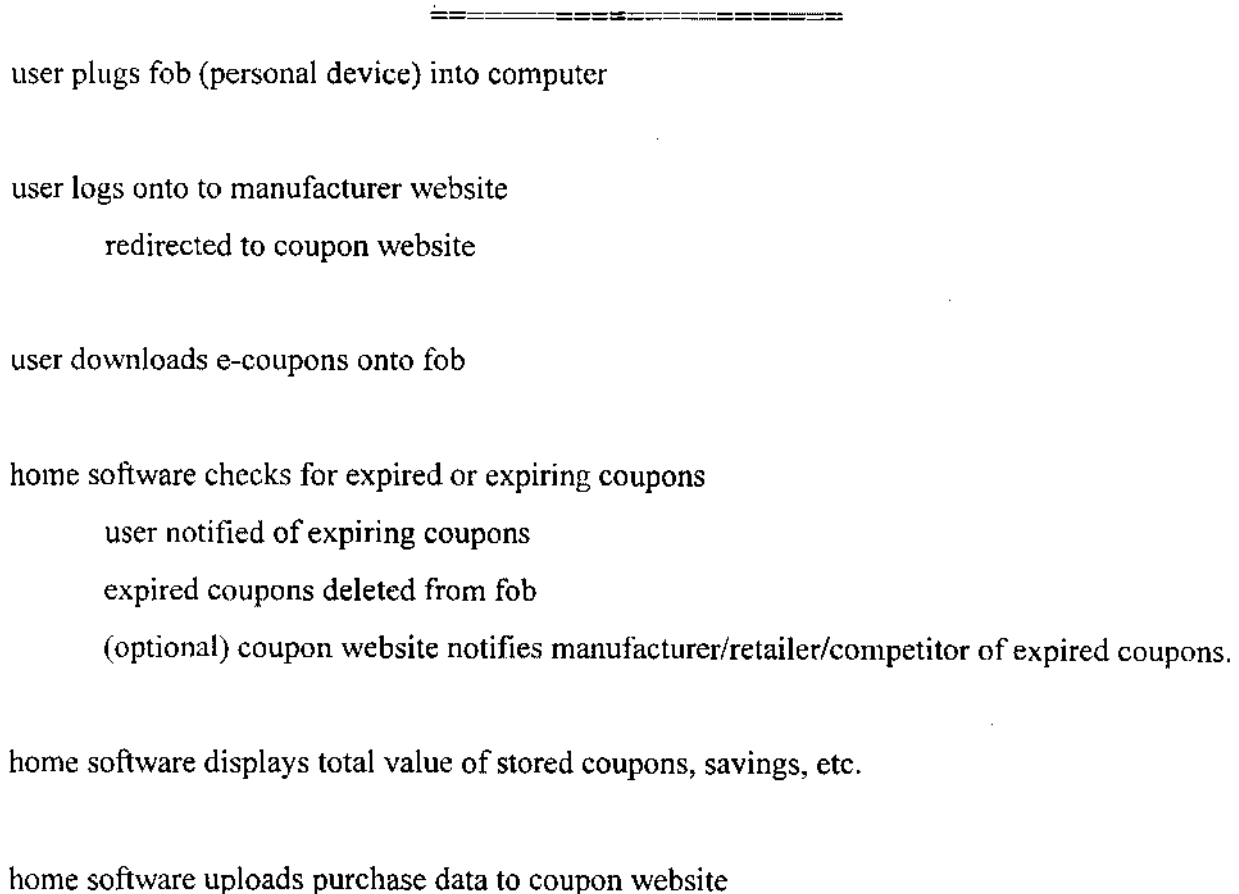
5) The home software would also allow the consumer to see the total value of coupons stored on the fob, total by product or category and a total of the redeemed coupons or actual savings.

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".



(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 download 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 appliance.
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 appliance.

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

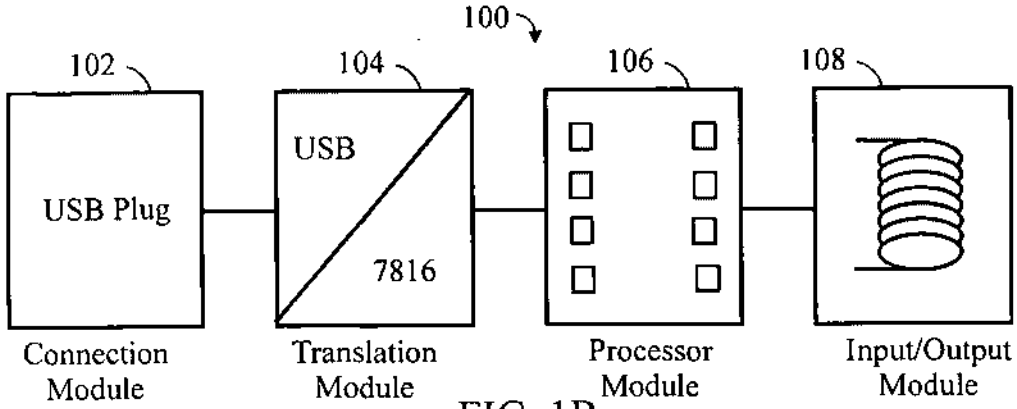


FIG. 1B

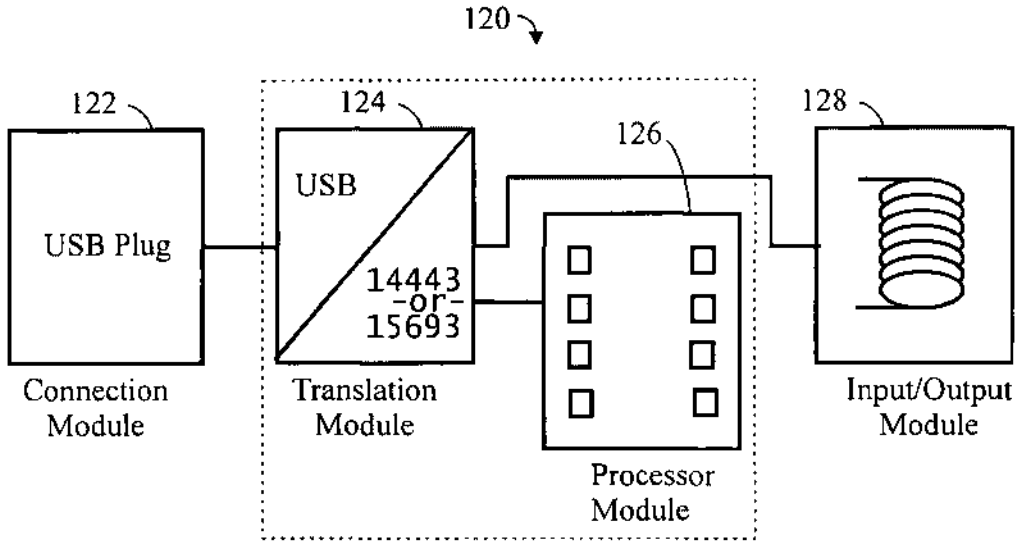
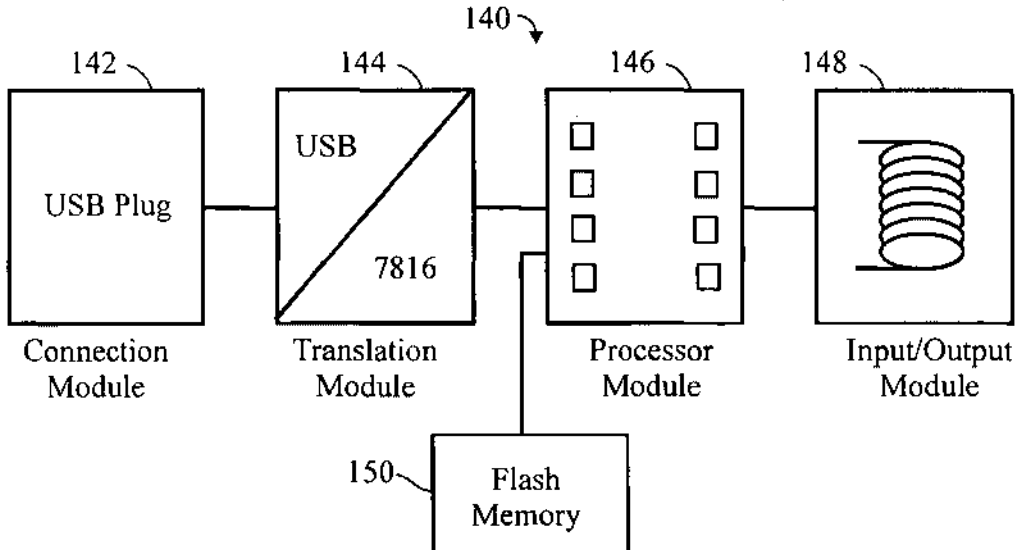
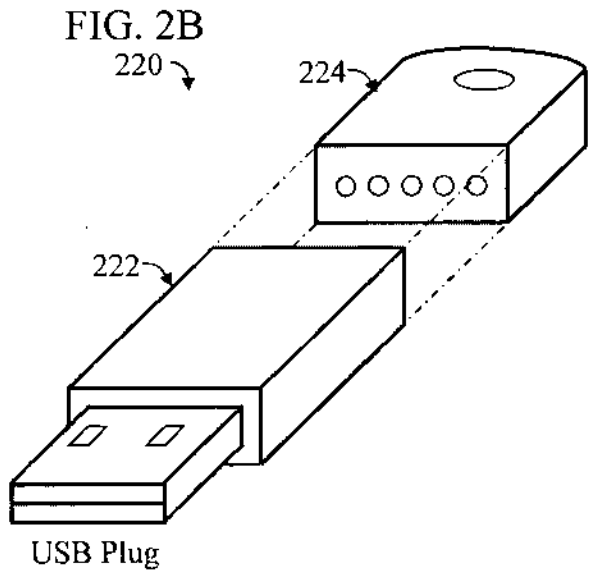
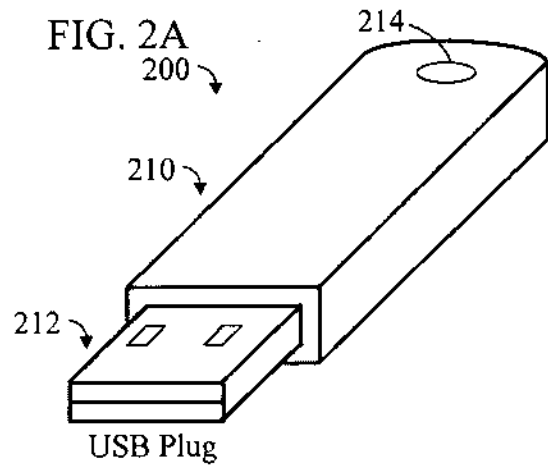


FIG 1C





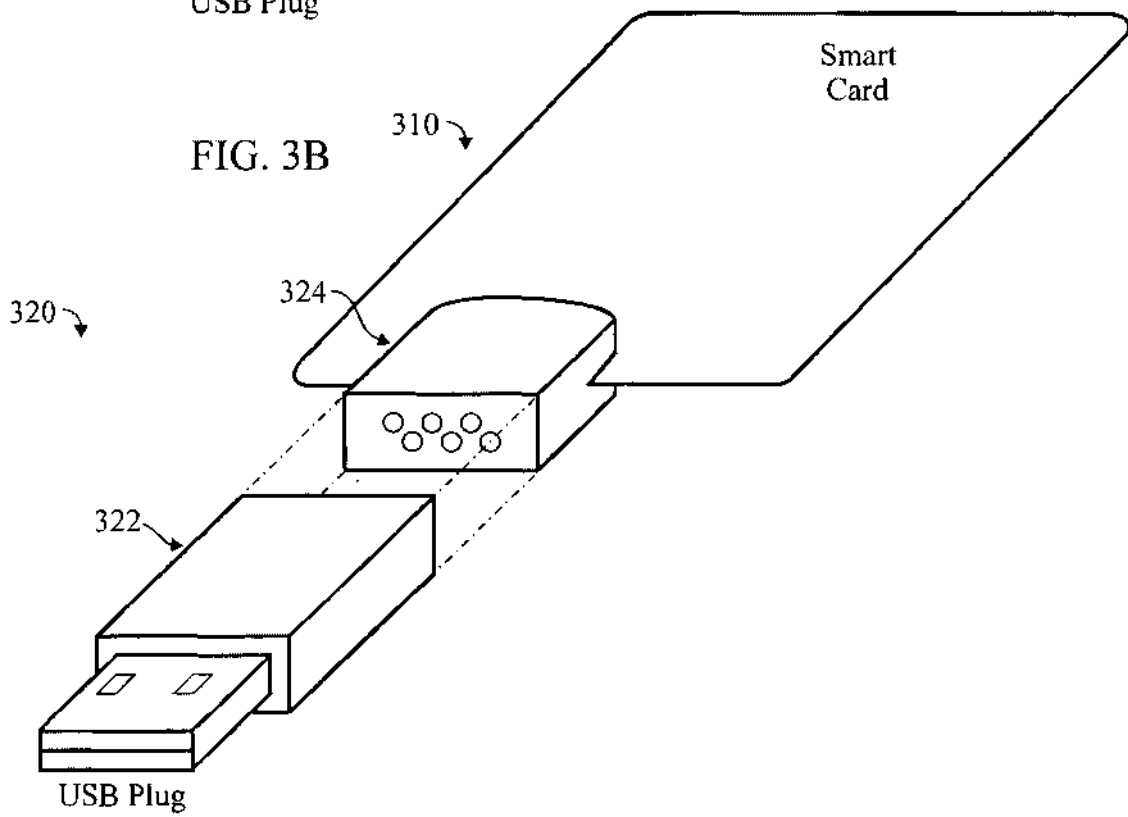
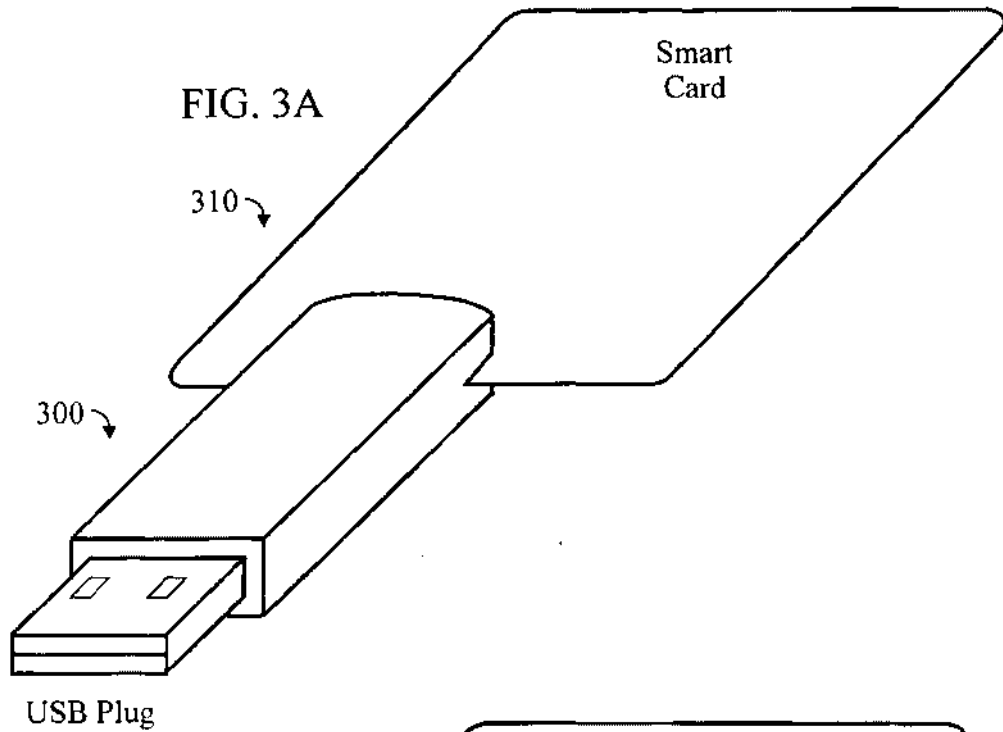


FIG 4

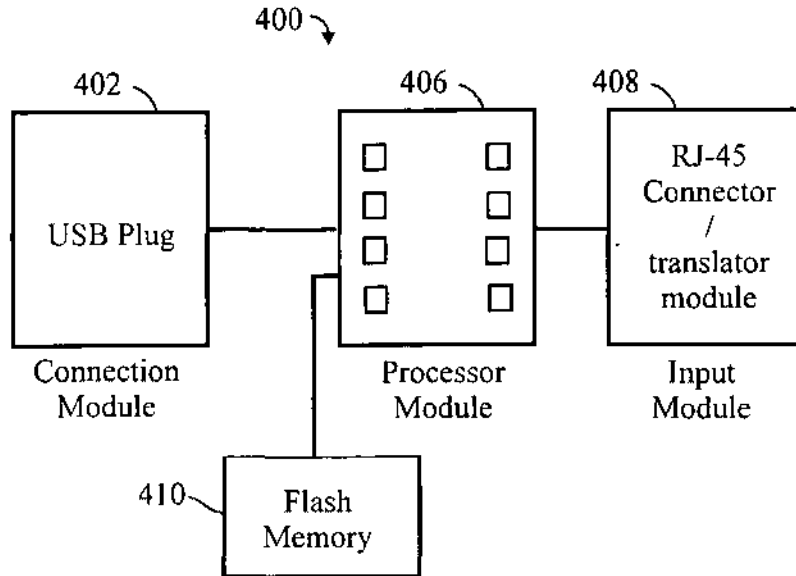
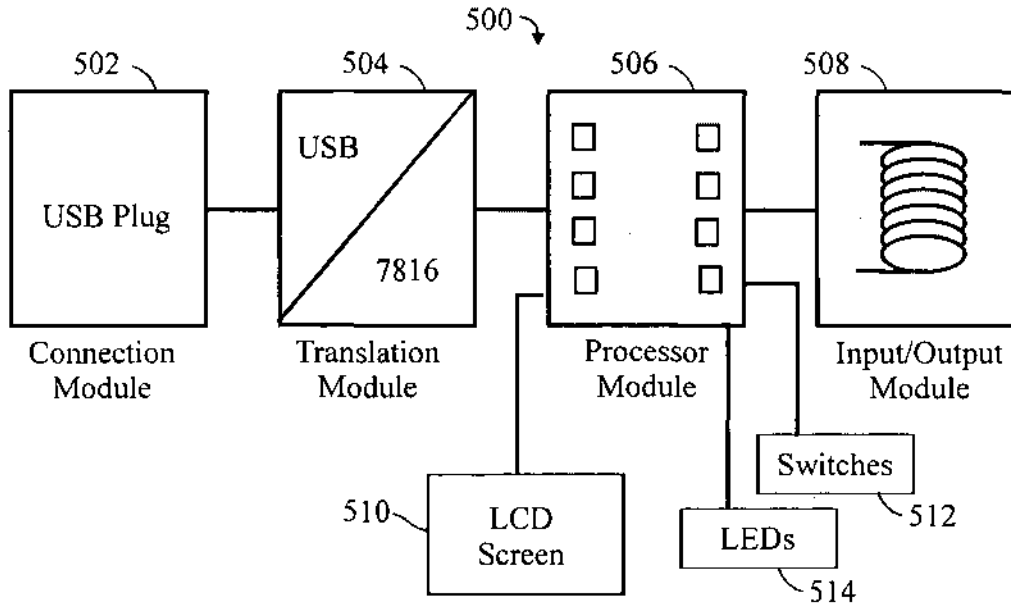


FIG 5



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

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.

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

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

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

\_\_\_\_\_  
Norbert Knapich                              Date                        Germany   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 <input type="checkbox"/>		

SMALL ENTITY TYPE

OR OTHER THAN SMALL ENTITY

RATE	FEE
BASIC FEE	395
X\$ 25=	800
X100=	
+180=	
TOTAL	1195

RATE	FEE
BASIC FEE	790
X\$50=	
X200=	
+360=	
TOTAL	

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

**CLAIMS AS AMENDED - PART II**

	(Column 1)	(Column 2)	(Column 3)
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total *	Minus **	=
	Independent *	Minus ***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <input type="checkbox"/>			

SMALL ENTITY OR

OTHER THAN SMALL ENTITY

RATE	ADDITIONAL FEE
X\$ 25=	
X100=	
+180=	
TOTAL ADDIT. FEE	

RATE	ADDITIONAL FEE
X\$50=	
X200=	
+360=	
TOTAL ADDIT. FEE	

	(Column 1)	(Column 2)	(Column 3)
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total *	Minus **	=
	Independent *	Minus ***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <input type="checkbox"/>			

RATE	ADDITIONAL FEE
X\$ 25=	
X100=	
+180=	
TOTAL ADDIT. FEE	

RATE	ADDITIONAL FEE
X\$50=	
X200=	
+360=	
TOTAL ADDIT. FEE	

	(Column 1)	(Column 2)	(Column 3)
AMENDMENT C	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total *	Minus **	=
	Independent *	Minus ***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <input type="checkbox"/>			

RATE	ADDITIONAL FEE
X\$ 25=	
X100=	
+180=	

RATE	ADDITIONAL FEE
X\$50=	
X200=	
+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**

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

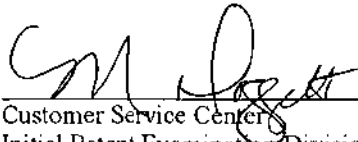
- **\$395** Statutory basic filing fee.
- **\$65** Late oath or declaration Surcharge.
- Total additional claim fee(s) for this application is **\$800**
  - **\$800** for **32** total claims over 20.



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

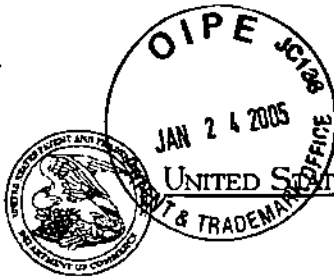
---

*A copy of this notice **MUST** 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

## 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

01/27/2005 DTESSEH1 00000082 10990296

01 FC:2001	395.00 DP
02 FC:2051	65.00 DP
03 FC:2202	800.00 DP

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 **MUST** 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:

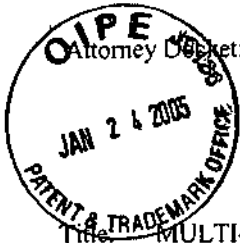
GERALD E. LINDEN  
12925 LA ROCHELLE CR.  
PALM BEACH GARDENS, FL 33410

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, 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 Corniskey, 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

Code 3, 18 of any international patent applications listed below:
date of the 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.



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.

[Signature] 1/29/04 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

[Signature] 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 1/2



Declaration of Ryan, et al. page 2/2

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

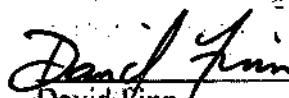
Inventor(s): Ryan, et al.

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.

		<u>US</u>
<u>Dennis J. Ryan</u>	<u>Date</u>	<u>Citizenship</u>
<u>2739 E Virgo Place</u>	<u>Chandler, AZ 85249</u>	
<u>Residence and Post Office Address</u>		

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

		<u>US</u>
<u>Patrick R. Comiskey</u>	<u>Date</u>	<u>Citizenship</u>
<u>2408 Edgerton Road</u>	<u>University Heights, Ohio 44118</u>	
<u>Residence and Post Office Address:</u>		

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





JAW

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 3/5/05  
Gerald E. Linden, Reg/ 30,282 date  
(561) 694-2094

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	6745267
6128673	6061746
6343364	6061746
6883715	5841471
6131125	5890016
6370603	5930496
6567273	5933656
6628325	5951667
6694399	5963726
6750902	5970220
6752321	5987106
6769622	6073188
6772956	6085156
6843423	6105143
6910638	6178458
6098171	6192420
6151647	6199122
6168077	6206480
6199128	6217389
6581122	6223134
6634565	6217389
6738259	6223134
6763399	6243778
6779059	6246578
6801956	6251014
6817534	6270415
6883718	6289405
6598032	6292863
6748541	6301104
6779734	6343260
6874680	6356968
6543690	6405145
6783078	6418392
6793144	6424525
6913196	6443839
6914695	6449662
6205505	6480801
5875313	6524137
5937175	6525932
5953511	6546441
5968142	6557754
6058441	6581123
6125409	6607139
6286063	6614708
6385677	6651184
6625472	6654841
6629181	6676420
6658516	6712698
6731751	6722985
6738856	6736678

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
----	-----	-----------------------	---	----	----	------------------



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  
CLEVELAND 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.

AK

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

Art Unit: 2876

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 --.



Art Unit: 2876

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

Art Unit: 2876

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

Art Unit: 2876

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

Art Unit: 2876

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 negated 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

Art Unit: 2876

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.

Art Unit: 2876

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



<b>Notice of References Cited</b>	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	Learning, 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.

<b>Notice of References Cited</b>	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-6,876,420 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.

COPYRIGHT: (C)2004,JPO&NCIPI

(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. <sup>7</sup>	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 O L (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 達  
 (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

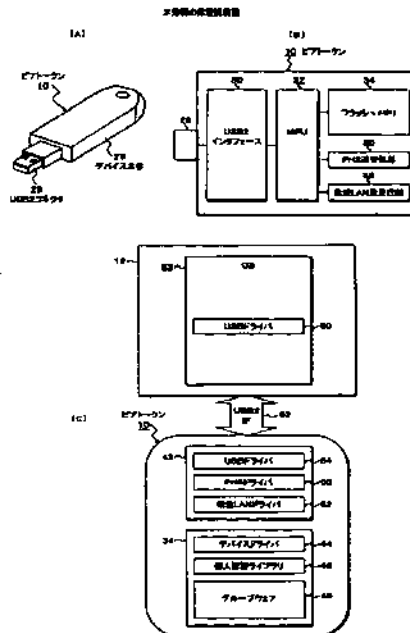
(54) 【発明の名称】 情報処理デバイス、情報処理方法及びプログラム

(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 [ピー・エニウェア]”、[平成15年2月3日検索]、インターネット<URL : [HYPERRLINK http://beemail.jp/anywhere.html](http://beemail.jp/anywhere.html) URL : <http://www.beemail.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

10

20

30

40

50

・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。

10

【0009】

一方、メモリスティ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。

20

【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。

30

40

【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。

50

## 【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。

10

## 【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。

20

## 【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。

30

## 【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つては、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。

40

## 【0023】

本発明の別の形態にあつては、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】

50



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。

10

## 【0032】

このようなピアトークン10の使用環境にあつては、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。

20

## 【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。

30

## 【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。

40

## 【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

50

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。

10

【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し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。

20

【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。

30

【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。

40

【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。

50

## 【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】

10

20

30

40

50

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側にあつては、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にあつては、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にあつては、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にあつては、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にあつては、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。 10

## 【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。 20

## 【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。 30

## 【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。 40

## 【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ます。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ります。

## 【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 50

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しようとする、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64に送る。

【0087】

これを受けて携帯電話64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

10

20

30

40

50

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側にあつては、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にあつ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、

10

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実行して実行させ、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)

20

【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。

30

【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)

40

【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】

50

## (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優すことなく、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

10

20

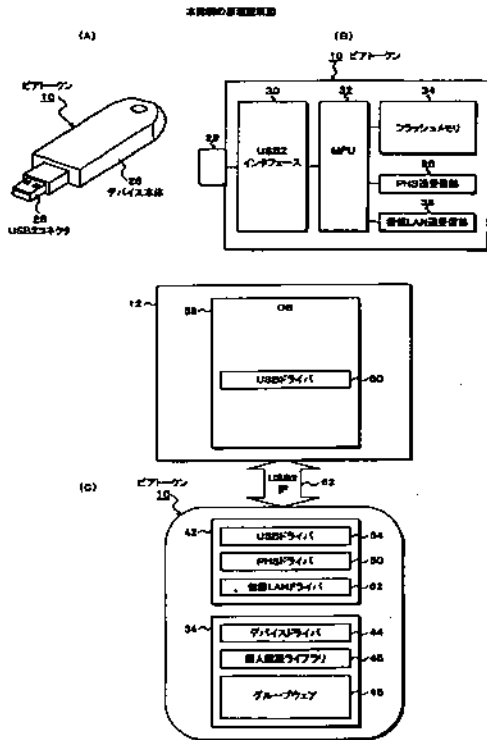
30

40

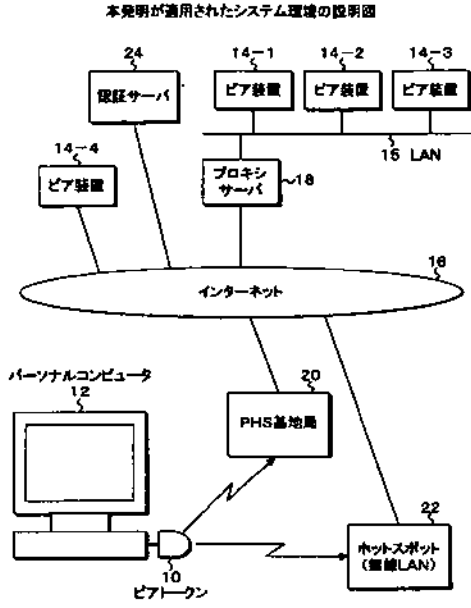
50

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)	10
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	20
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	30

【図1】

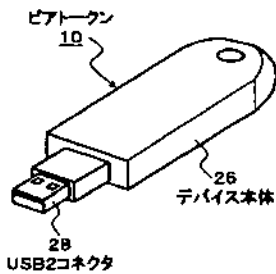


【図2】



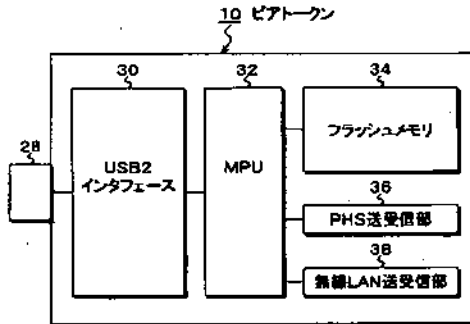
【図3】

本発明によるキー型ピアトークンの外観の説明図



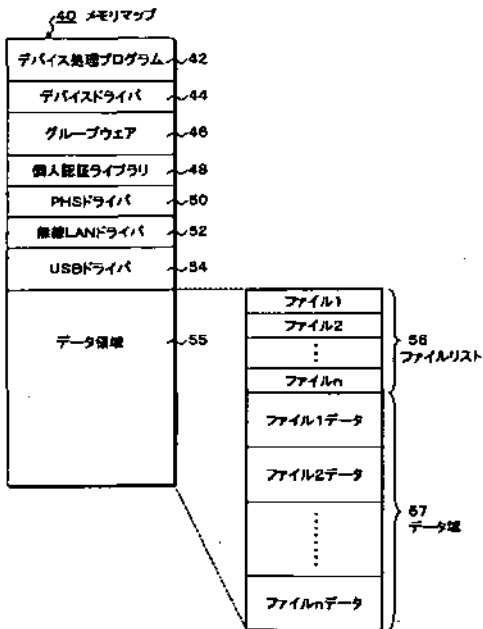
【図4】

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



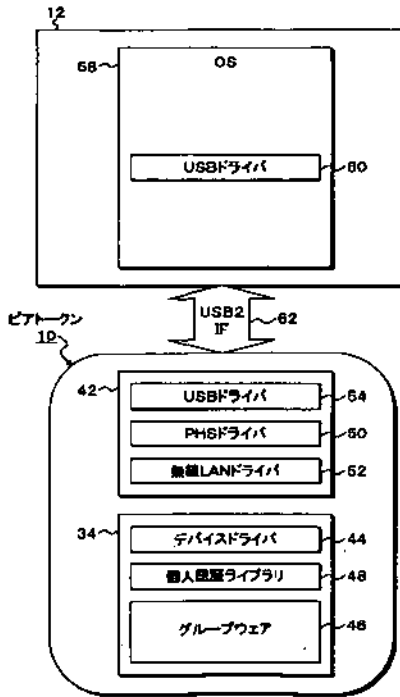
【図5】

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



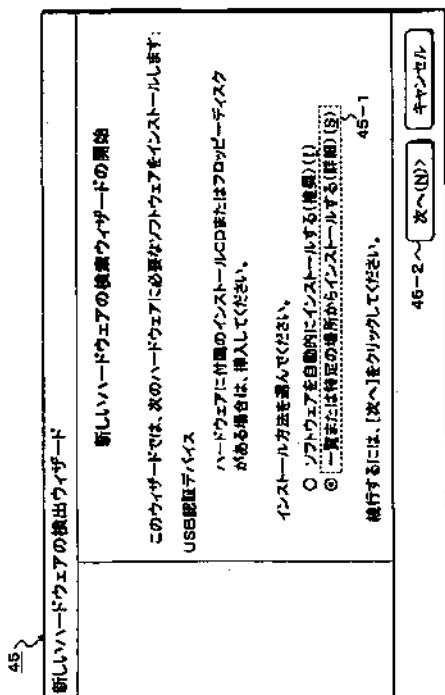
【図6】

本発明のピアトゥー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



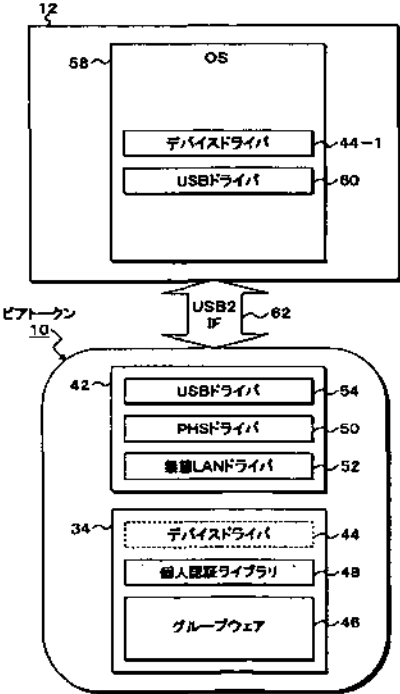
【図7】

ピアトゥー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



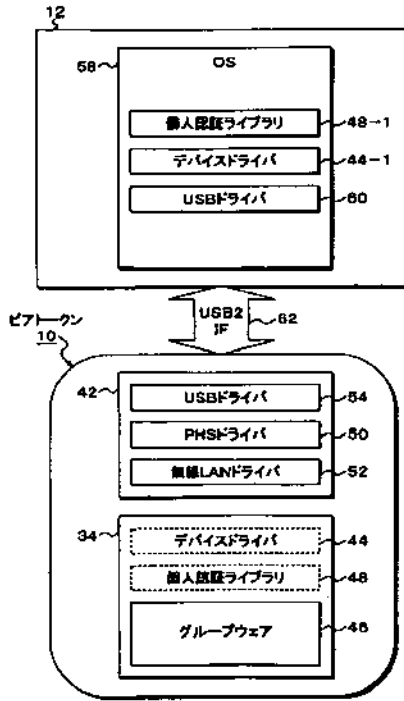
【図8】

図8に示し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



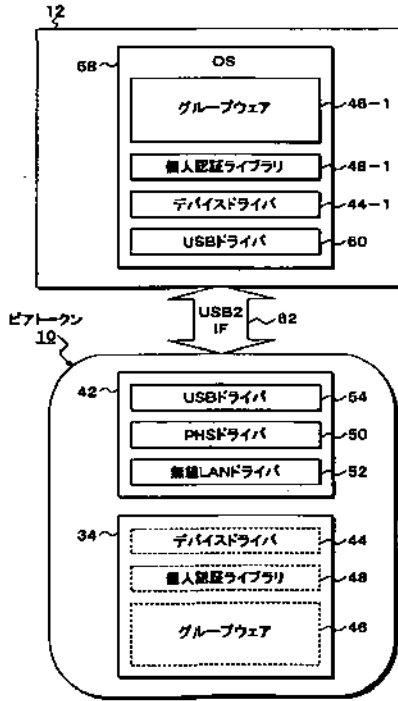
【図9】

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



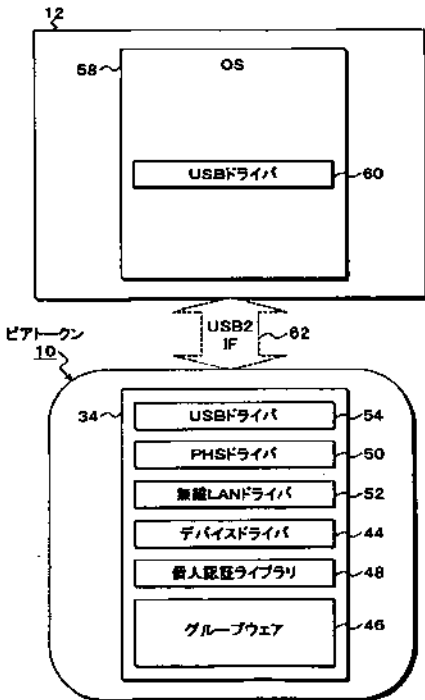
【図10】

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



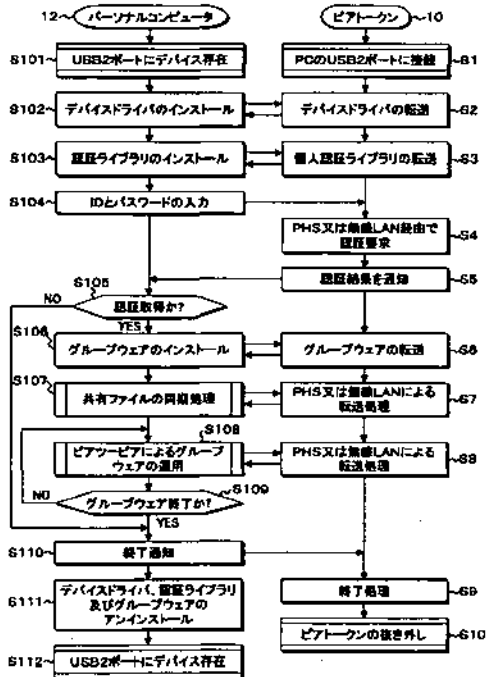
【図11】

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ンを外した際の説明図



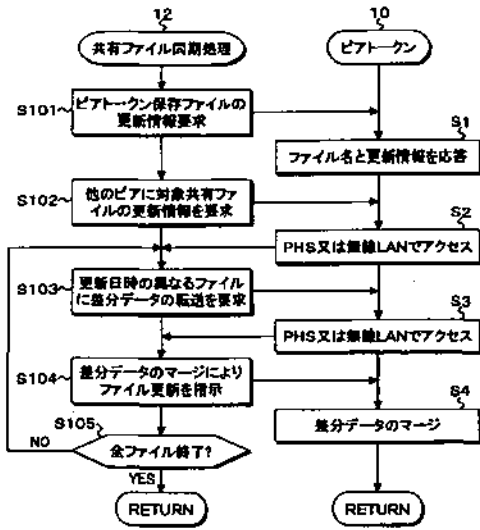
【図12】

本発明のピアトー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



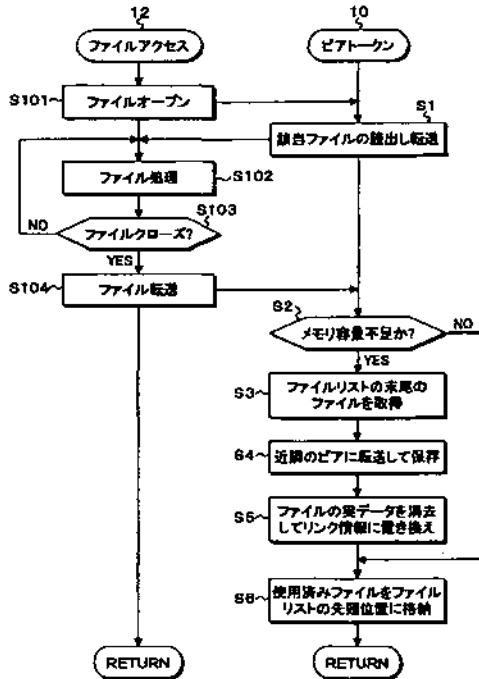
【図13】

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



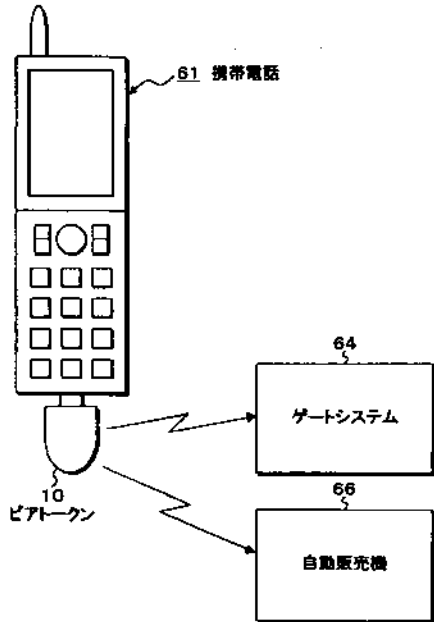
【図14】

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



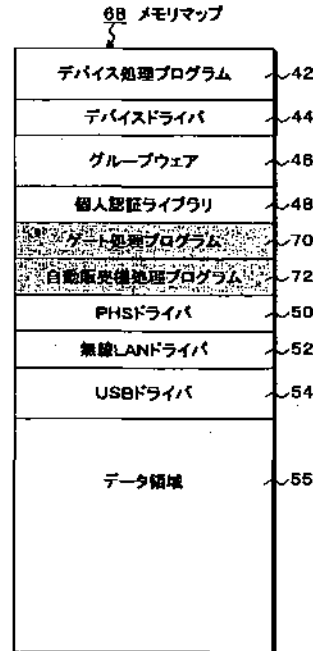
【図15】

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】

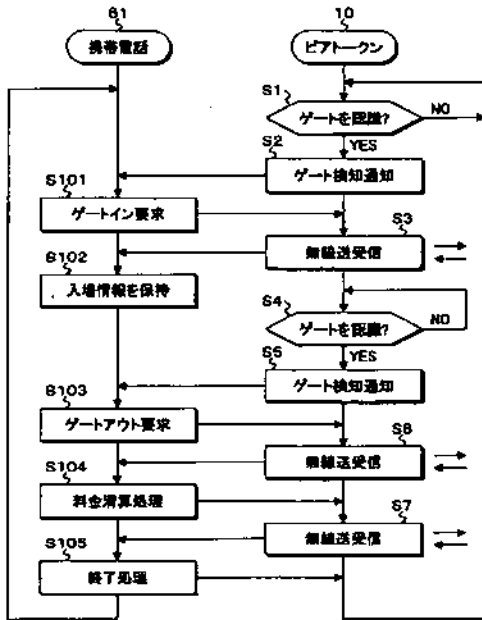
図6のピアトークンにおける不揮発メモリのメモリマップ説明図





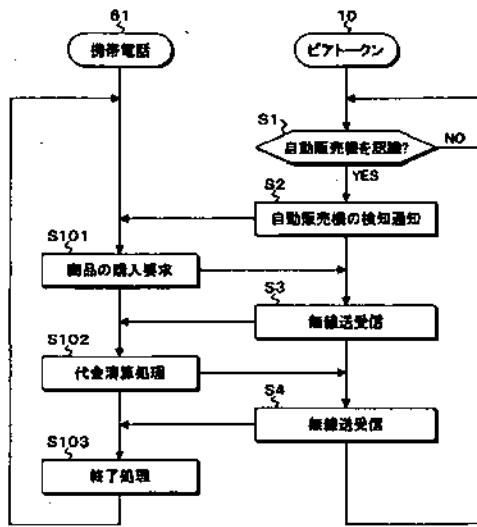
【図17】

ゲートシステムを対象とした本発明のピアトゥー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ゥー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.<sup>7</sup>

F I

テーマコード (参考)

G 0 6 F 9/06 6 6 0 E

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

(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 Classification<sup>7</sup>: 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). ANDER-  
SON, Allan, D.; 11158 Bertha Place, Cerritos, CA 90703

(US). GODDING, Patrick, N.; 22665 Shady Grove Cir-  
cle, Lake Forest, CA 92630 (US). PUNT, Maarten, G.;  
24942 Paseo Arboleda, Lake Forest, CA 92630 (US). SO-  
TOODEH, Mehdi; 17 Paloma Drive, Mission Viejo, CA  
92692 (US).

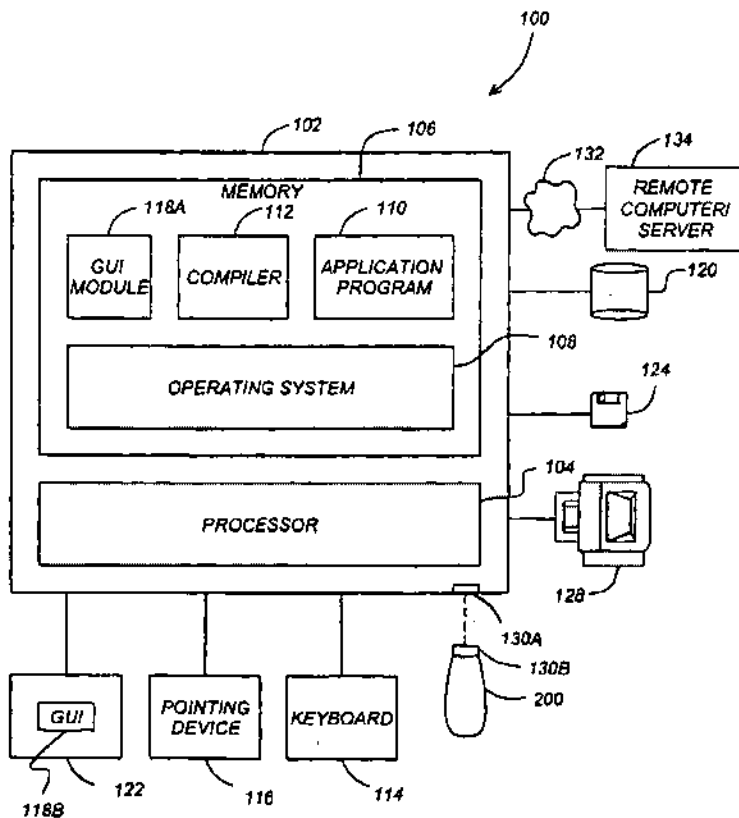
(74) Agents: SMITH, Samuel, Leonard et al.; J.A. Kemp &  
Co., 14 South Square, Gray's Inn, London WC1R 5JJ (GB).

(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 EM-  
ULATOR



(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).

*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.*

**Published:**

— *without international search report and to be republished upon receipt of that report*

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, Bahram 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.

25

#### 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)

#### 15 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;

20 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

25 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  
5 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  
10 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  
15 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  
20 112 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  
25 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, 5 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 10 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 15 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 20 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, 25 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  
5 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  
10 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  
15 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 actuable 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  
20 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  
25 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.

5           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  
10           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  
15           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.

20           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  
25           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

5 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  
10 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  
15 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  
20 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  
25 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)

5

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-  
5 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  
10 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  
15 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  
20 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  
25 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  
5 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  
10 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  
15 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.

20 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)  
25 302. 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.

5           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.

15           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.

20           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

5

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

5

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

10

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);
  - 5 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
  - 10 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.
- 15 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
  - 20 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
  - 25 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.

10

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.

15

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).

20

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:

25

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;

5 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);

10 accepting a smartcard response from the smartcard processor (320);

translating the smartcard response into a smartcard reader response;

15 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);

20 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  
5 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);  
10 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  
15 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:  
20 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).

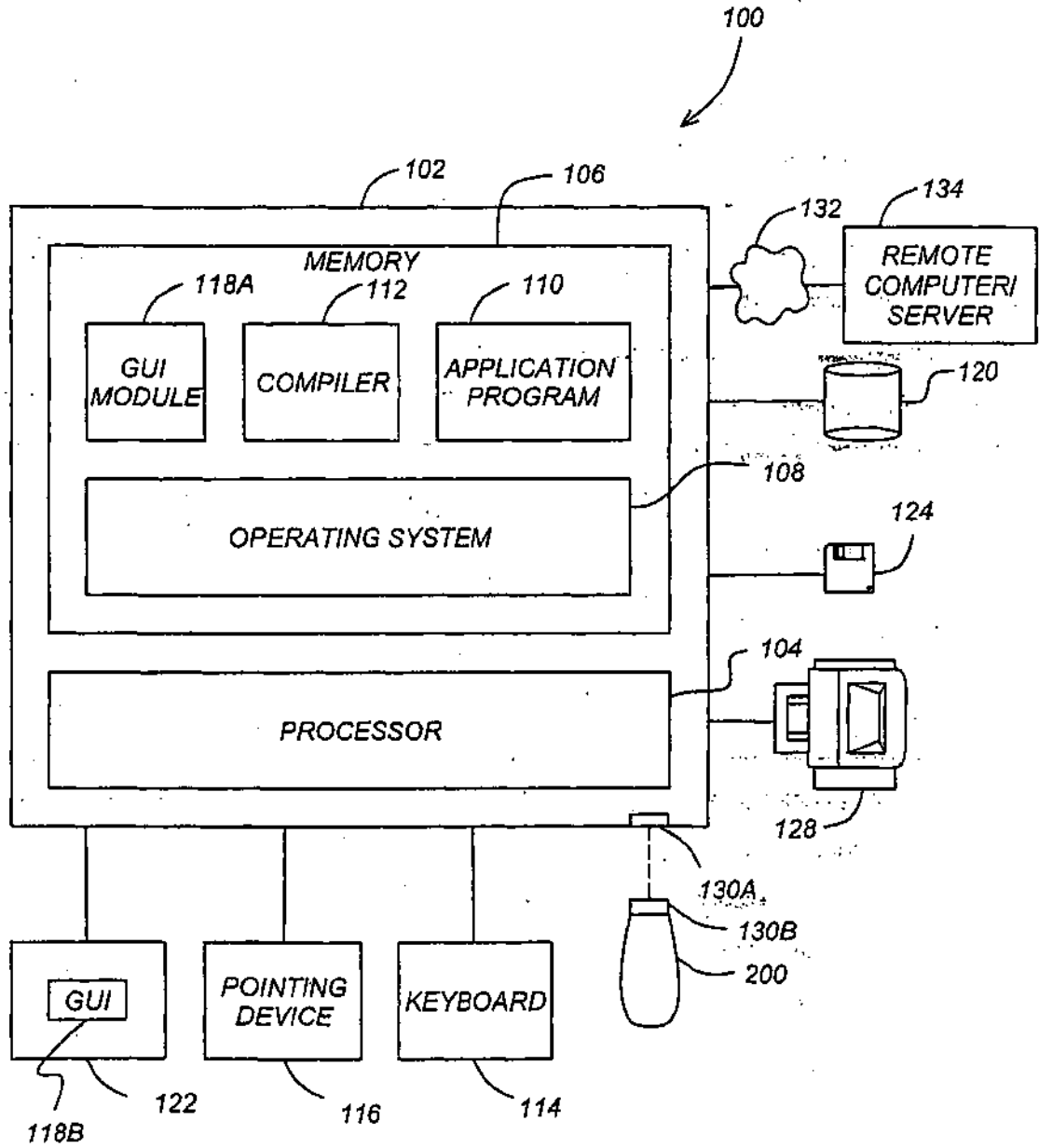


FIG. 1

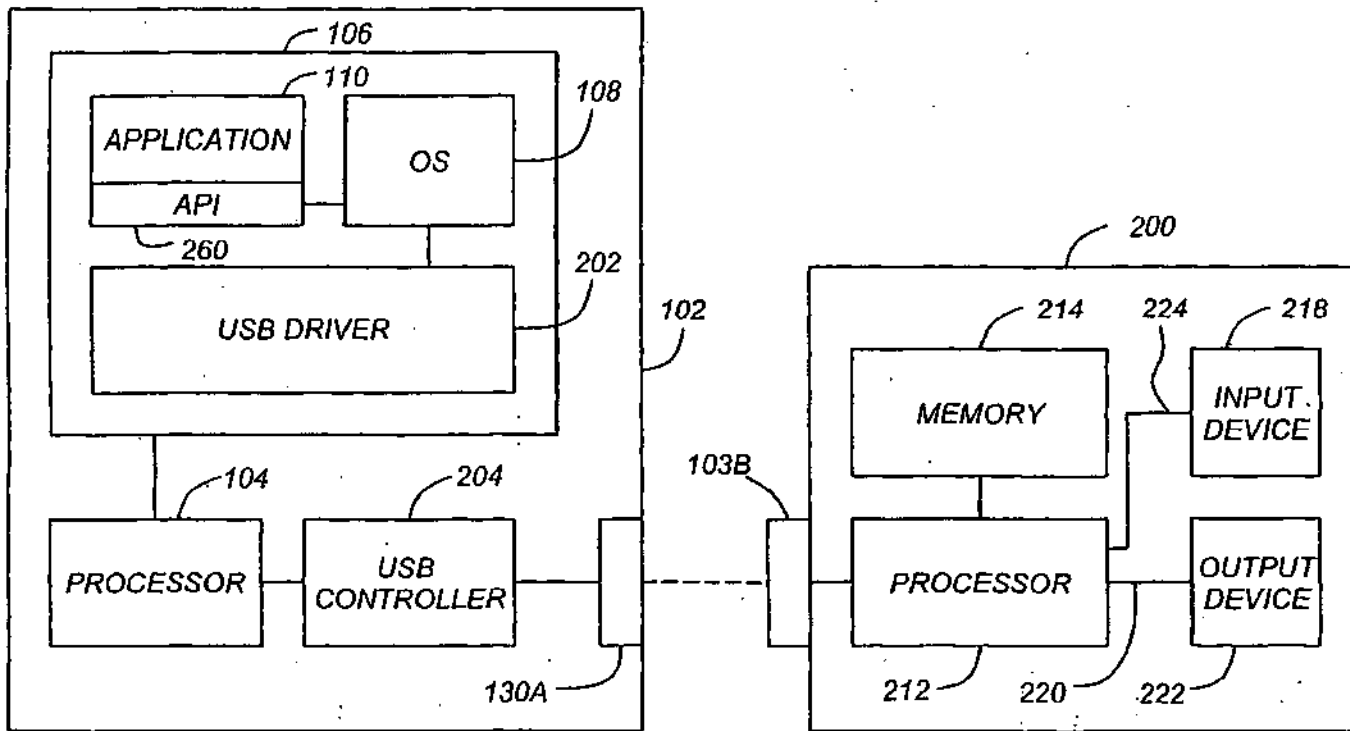


FIG. 2

2/7

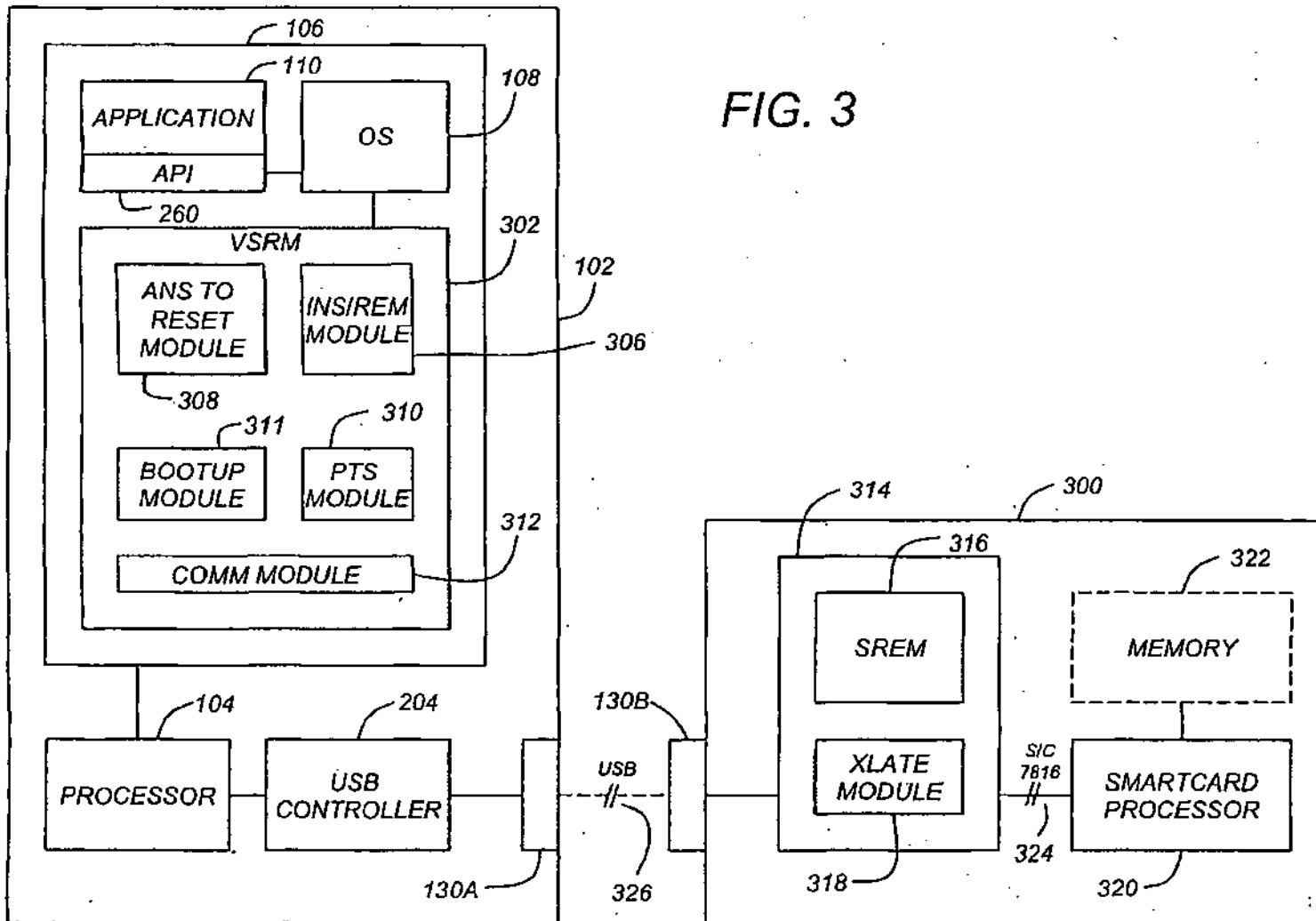


FIG. 3

3/7

4/7

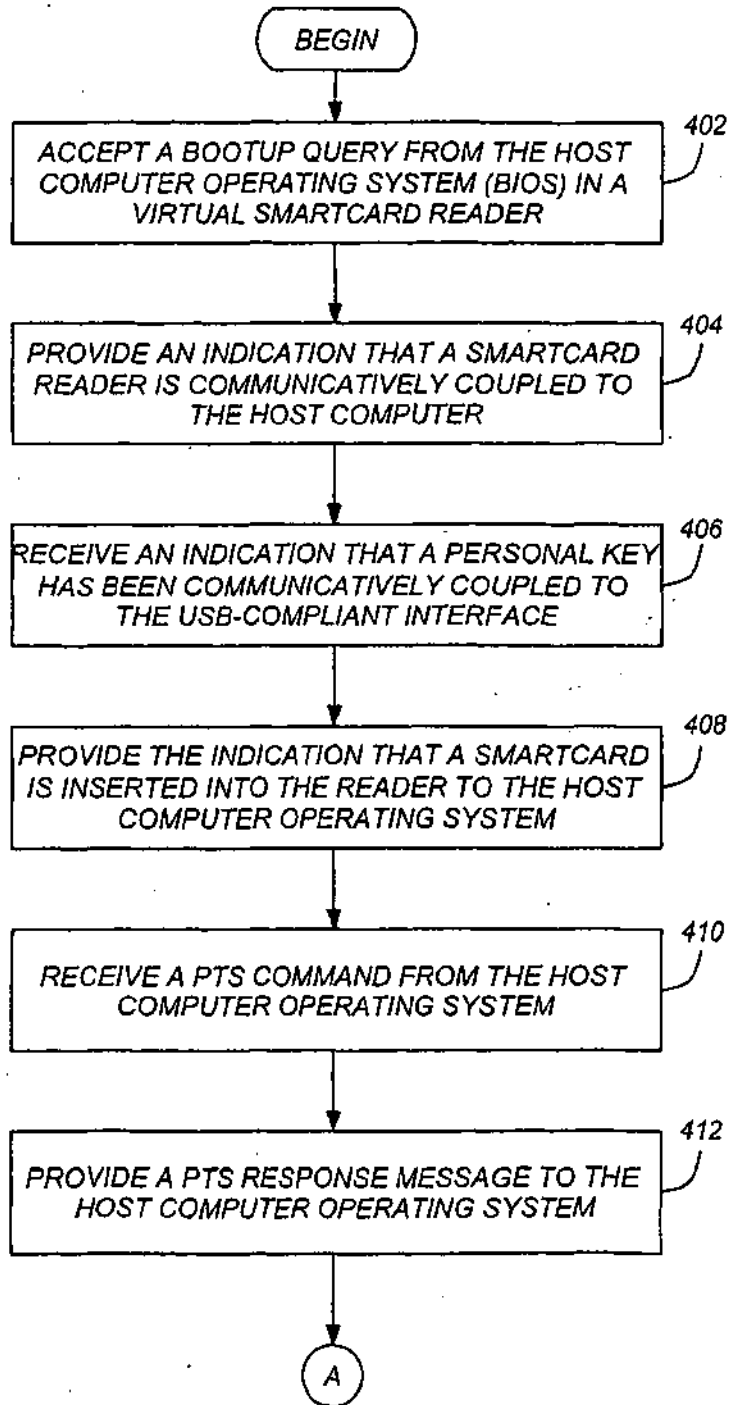
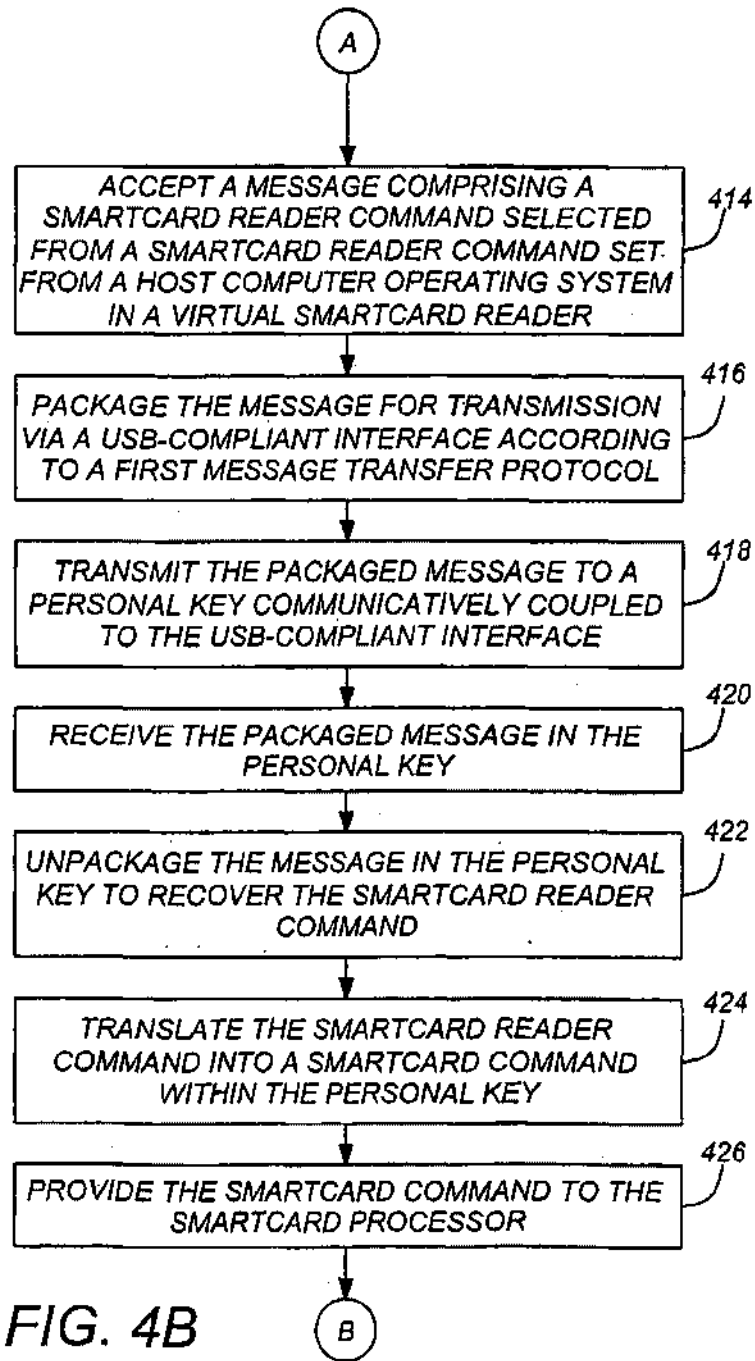


FIG. 4A



5/7



6/7

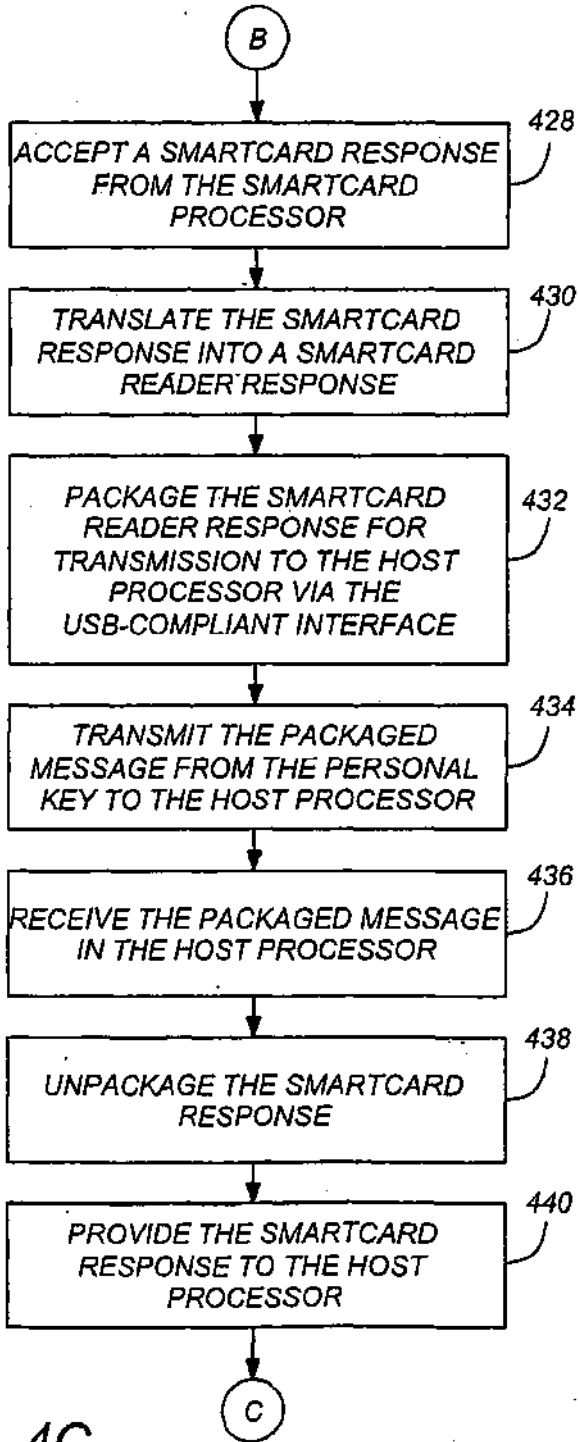


FIG. 4C

7/7

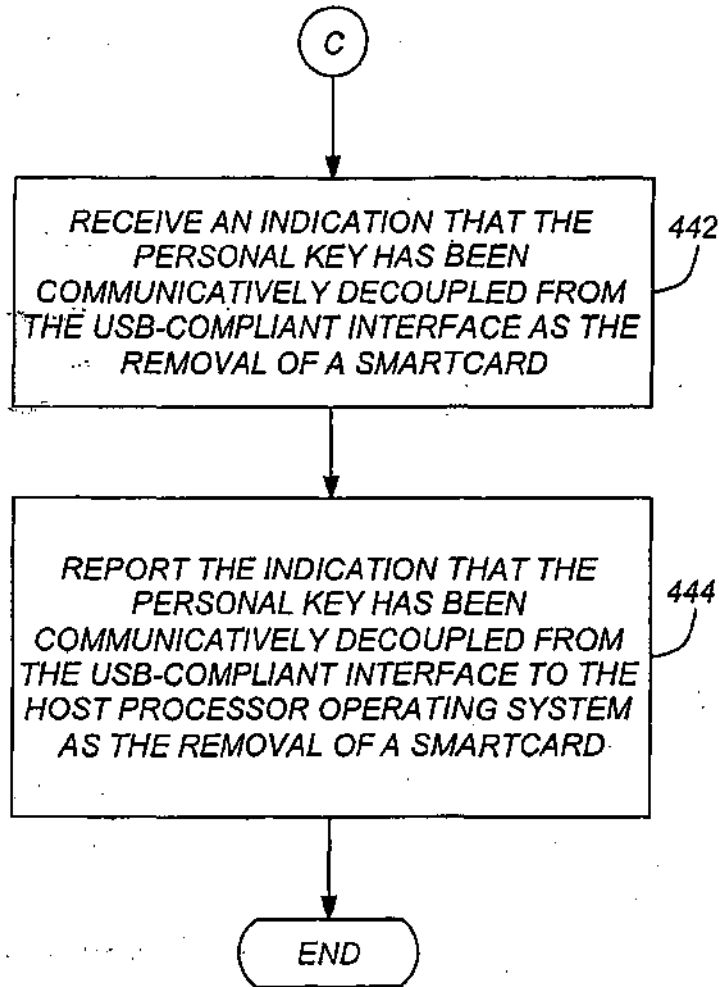


FIG. 4D



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 \*\*\*\*\* *Ull*  
 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 \*\*\*\*\* *Ull*

IF REQUIRED, FOREIGN FILING LICENSE GRANTED \*\* SMALL ENTITY \*\* *Ull*  
 \*\* 12/16/2004

Foreign Priority claimed 35 USC 119 (a-d) conditions met Verified and Acknowledged	<input type="checkbox"/> yes <input checked="" type="checkbox"/> no <input type="checkbox"/> yes <input checked="" type="checkbox"/> no <input type="checkbox"/> Met after Allowance Examiner's Signature <i>Ull</i> 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  
 CLEVELAND HTS. , OH  
 44121-2016

TITLE  
 Multi-interface compact personal token apparatus and methods of use

FILING FEE	FEES: Authority has been given in Paper	<input type="checkbox"/> All Fees <input type="checkbox"/> 1.16 Fees ( Filing ) <input type="checkbox"/> 1.17 Fees ( Processing Ext. of time )
------------	---	--

**Index of Claims**



Application/Control No.

10/990,296

Examiner

Uyen-Chau N. Le

Applicant(s)/Patent under Reexamination

RYAN ET AL.

Art Unit

2876

√	Rejected
=	Allowed

-	(Through numeral) Cancelled
+	Restricted

N	Non-Elected
I	Interference

A	Appeal
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	√			

Claim		Date			
Final	Original	7/7/05			
	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

Examiner

Uyen-Chau N. Le

Applicant(s)/Patent under Reexamination

RYAN ET AL.

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



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.

<b>TRANSMITTAL FORM</b>  <i>(to be used for all correspondence after initial filing)</i>	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	
Total Number of Pages in This Submission	6	Attorney Docket Number	Ryan C-4

ENCLOSURES (Check all that apply)		
<input checked="" type="checkbox"/> Fee Transmittal Form	<input type="checkbox"/> Drawing(s)	<input type="checkbox"/> After Allowance Communication to TC
<input checked="" type="checkbox"/> Fee Attached	<input type="checkbox"/> Licensing-related Papers	<input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences
<input type="checkbox"/> Amendment/Reply	<input type="checkbox"/> Petition	<input type="checkbox"/> Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
<input type="checkbox"/> After Final	<input type="checkbox"/> Petition to Convert to a Provisional Application	<input type="checkbox"/> Proprietary Information
<input type="checkbox"/> Affidavits/declaration(s)	<input type="checkbox"/> Power of Attorney, Revocation	<input type="checkbox"/> Status Letter
<input type="checkbox"/> Extension of Time Request	<input type="checkbox"/> Change of Correspondence Address	<input checked="" type="checkbox"/> Other Enclosure(s) (please identify below):
<input type="checkbox"/> Express Abandonment Request	<input type="checkbox"/> Terminal Disclaimer	<b>RECEIPT POSTCARD</b>
<input checked="" type="checkbox"/> Information Disclosure Statement	<input type="checkbox"/> Request for Refund	
<input type="checkbox"/> Certified Copy of Priority Document(s)	<input checked="" type="checkbox"/> CD, Number of CD(s) <u>1</u>	
<input type="checkbox"/> Reply to Missing Parts/Incomplete Application	<input type="checkbox"/> Landscape Table on CD	
<input type="checkbox"/> Reply to Missing Parts under 37 CFR 1.52 or 1.53	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 ADOBE ACROBAT READER (PDF) FORMAT IN THE ENCLOSED CD.	

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT			
Firm Name	D.A. STAUFFER PATENT SERVICES LLC		
Signature			
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			
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 and 1.14. 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.



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.  
As amended by the Consolidated Appropriations Act, 2005 (H.R. 4818).

# FEE TRANSMITTAL

## For FY 2005

**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

Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT (\$) 180

**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**

Application Type	FILING FEES		SEARCH FEES		EXAMINATION FEES		Fees Paid (\$)
	Fee (\$)	Small Entity Fee (\$)	Fee (\$)	Small Entity Fee (\$)	Fee (\$)	Small Entity Fee (\$)	
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 (\$)	Multiple Dependent Claims	Fee (\$)	Fee Paid (\$)
_____ - 20 or HP = _____	x _____	= _____	_____	_____	_____	_____

HP = highest number of total claims paid for, if greater than 20.

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)**

Non-English Specification, \$130 fee (no small entity discount) Fees Paid (\$)  
 Other (e.g., late filing surcharge): Submission of IDS after first Office Action 180

**SUBMITTED BY**

Signature	<i>D. Stauffer</i>	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.





substitute forms PTO/SB/08a, PTO/SB/08b  <b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>	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 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  <b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>	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 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	<i>ACR38CT Contactless SIM Tracker Technical Specification</i> , Advanced Card Systems Ltd., Hong Kong.	T
	2	<i>ACR38DT Dual Key Technical Specifications, Version 1.3</i> , September 2004, Advanced Card Systems Ltd., Hong Kong.	T
	3	<i>Dallas Semiconductor DS1490F 2-in-1 Fob</i> , Dallas Semiconductor, Dallas TX.	T

substitute forms PTO/SB/08a & PTO/SB/08b  <b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>	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	<i>Dallas Semiconductor DS9490-DS9490R USB to 1-Wire/iButton Adaptor</i> , Maxim I-C, Sunnyvale CA.	T
	5	HARA, YOSHIKO, <i>Matsushita blends FERAM technology with smart cards</i> , October 1, 2004, CMP Media, Manhasset NY.	T
	6	<i>Japan's Matsushita developing memory cards with smart chip function</i> , October 1, 2004, Mercury News, San Jose CA.	T
	7	<i>OTi-6828 Flash Disk Controller</i> , Ours Technology Inc., Taiwan.	T
	8	<i>Panasonic Develops RFID smartSD Card</i> , October 4, 2004, Palminfocenter.com, Sunnyvale CA.	T
	9	<i>Panasonic Develops Industry's First SD Memory Card with Contactless Smart Card Capabilities</i> , October 1, 2004, The Japan Corporate News Network, Tokyo.	T
	10	ROJAS, PETER, <i>Panasonic's Smart SD adds RFID to the mix</i> , October 4, 2004, Engadget LLC, New York NY.	T
	11	<i>Delivering ultimate security, high performance and ultra low power consumption, SmartMX is now in volume supply</i> , November 18-20, 2003, Cartes 2003, aris Nort Villepinte, France	T
	12	BALABAN, DAN, <i>Digital Rights pits SIMS against Flash Cards</i> , <i>Card Technology</i> , November 2004, pp 24-30, Card Technology, Chicago IL.	T
	13	<i>P5CT072 Secure Dual Interface PKI Smart Card Controller, Rev. 1.3</i> , October 2004, Koninklijke Philips Electronics, The Netherlands	T
	14	<i>Vodafone KK Develops Contactless Smart Card Mobile Handset</i> , May 6, 2004, HITEK Magazine, Dubai	T
	15	<i>SmartSD Card Structure</i>	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

10990296 UK

Indicate quantity of a single type of artifact received but not scanned. Create individual artifact folder/box and artifact number for each Artifact Type.

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

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

**RECEIVED  
CENTRAL FAX CENTER**

NOV 14 2005

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.

11/16/2005 TL0111 00000043 10990296

01 FC:2251

60.00 OP

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 ~~appliance~~ 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 (RFID-contactless interface) and ISO 15693 (RFID-contactless interface).

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 releasably 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 ~~appliance~~  
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 A1). 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 connectable 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](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](http://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 JPEG, 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 throughout 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 802.11, 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 previous 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 802.11, 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.

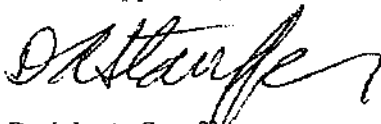
**Conclusion**

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

RECEIVED  
CENTRAL FAX CENTER

NOV 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.

<b>TRANSMITTAL FORM</b>  <small>(to be used for all correspondence after initial filing)</small>	Application Number	10/990,296
	Filing Date	11 / 16 / 2004
	First Named Inventor	Donnis J. Ryan
	Art Unit	2876
	Examiner Name	Uyen Chau N. Lu
	Attorney Docket Number	Ryan C-4
Total Number of Pages in This Submission		30

ENCLOSURES (Check all that apply)		
<input checked="" type="checkbox"/> Fee Transmittal Form	<input type="checkbox"/> Drawing(s)	<input type="checkbox"/> After Allowance Communication to TC
<input checked="" type="checkbox"/> Fee Attached	<input type="checkbox"/> Licensing-related Papers	<input type="checkbox"/> Appeal Communication to Board of Appeals and Interferences
<input checked="" type="checkbox"/> Amendment/Reply	<input type="checkbox"/> Petition	<input type="checkbox"/> Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
<input type="checkbox"/> After Final	<input type="checkbox"/> Petition to Convert to a Provisional Application	<input type="checkbox"/> Proprietary Information
<input type="checkbox"/> Affidavits/declaration(s)	<input type="checkbox"/> Power of Attorney, Revocation	<input type="checkbox"/> Status Letter
<input checked="" type="checkbox"/> Extension of Time Request	<input type="checkbox"/> Change of Correspondence Address	<input checked="" type="checkbox"/> Other Enclosure(s) (please identify below):
<input type="checkbox"/> Express Abandonment Request	<input type="checkbox"/> Terminal Disclaimer	PTO-2038 Credit Card Payment Form for payment of \$60 extension fee
<input type="checkbox"/> Information Disclosure Statement	<input type="checkbox"/> Request for Refund	
<input type="checkbox"/> Certified Copy of Priority Document(s)	<input type="checkbox"/> CD, Number of CD(s) _____	
<input type="checkbox"/> Reply to Missing Parts/ Incomplete Application	<input type="checkbox"/> Landscape Table on CD	
<input type="checkbox"/> Reply to Missing Parts under 37 CFR 1.52 or 1.53	Remarks	

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT			
Firm Name	D.A. STAUFFER PATENT SERVICES LLC		
Signature			
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			
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 and 1.14. 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.

**RECEIVED  
CENTRAL FAX CENTER**

NOV 14 2005

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**

Complete if Known

Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT (\$) 60

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**

Application Type	FILING FEES		SEARCH FEES		EXAMINATION FEES		Fees Paid (\$)
	Fee (\$)	Small Entity Fee (\$)	Fee (\$)	Small Entity Fee (\$)	Fee (\$)	Small Entity Fee (\$)	
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
<b>Total Claims</b>	<b>Extra Claims</b>	<b>Fee (\$)</b>
52 - 20 or HP = 0 x _____ = _____		
HP = highest number of total claims paid for, if greater than 20.		
<b>Indep. Claims</b>	<b>Extra Claims</b>	<b>Fee (\$)</b>
3 - 3 or HP = 0 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)**

Non-English Specification, \$130 fee (no small entity discount) Fees Paid (\$)

Other (e.g., late filing surcharge): one month extension of time fee 60

**SUBMITTED BY**

Signature	<i>Dwight A. Stauffer</i>	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 <input type="checkbox"/>		

SMALL ENTITY TYPE

OR OTHER THAN SMALL ENTITY

RATE	FEE
BASIC FEE	395
X\$ 25=	800
X100=	
+180=	
TOTAL	1195

RATE	FEE
BASIC FEE	790
X\$50=	
X200=	
+360=	
TOTAL	

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

11/19/05 **CLAIMS AS AMENDED - PART II**

	(Column 1)	(Column 2)	(Column 3)
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total	52 Minus	52 =
	Independent	3 Minus	3 =
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <input checked="" type="checkbox"/>			

SMALL ENTITY OR

OTHER THAN SMALL ENTITY

RATE	ADDITIONAL FEE
X\$ 25=	
X100=	
+180=	
TOTAL ADDIT. FEE	

RATE	ADDITIONAL FEE
X\$50=	
X200=	
+360=	
TOTAL ADDIT. FEE	

	(Column 1)	(Column 2)	(Column 3)
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total	* Minus	** =
	Independent	* Minus	*** =
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <input type="checkbox"/>			

RATE	ADDITIONAL FEE
X\$ 25=	
X100=	
+180=	
TOTAL ADDIT. FEE	

RATE	ADDITIONAL FEE
X\$50=	
X200=	
+360=	
TOTAL ADDIT. FEE	

	(Column 1)	(Column 2)	(Column 3)
AMENDMENT C	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
	Total	* Minus	** =
	Independent	* Minus	*** =
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <input type="checkbox"/>			

RATE	ADDITIONAL FEE
X\$ 25=	
X100=	
+180=	

RATE	ADDITIONAL FEE
X\$50=	
X200=	
+360=	

# CLAIMS ONLY

SERIAL NO. **181990296**  
 FILING DATE  
 APPLICATION

**11/14/05**

## CLAIMS

	AS FILED		AFTER 1st AMENDMENT		AFTER 2nd AMENDMENT									
	INC.	DER.	INC.	DER.	INC.	DER.		INC.	DER.	INC.	DER.	INC.	DER.	
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														
TOTAL INC.														
TOTAL DER.														
TOTAL CLAIMS														

\* MAY BE USED FOR ADDITIONAL CLAIMS OR AMENDMENTS

FORM PTO-2023 (1-06)

U.S. DEPARTMENT OF COMMERCE  
 Patent and Trademark Office

U.S. Government Printing Office: 1999 - 439-214/7000

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	33	("20010043702" "20010054148" "200200111516" "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 (wireless rf 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      01/25/2006

D.A. STAUFFER PATENT SERVICES LLC  
1006 MONTFORD ROAD  
CLEVELAND 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.



<b>Office Action Summary</b>	<b>Application No.</b> 10/990,296	<b>Applicant(s)</b> RYAN ET AL.	
	<b>Examiner</b> Uyen-Chau N. Le	<b>Art Unit</b> 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: \_\_\_\_\_

Art Unit: 2876

**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.

Art Unit: 2876

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

Art Unit: 2876

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,

Art Unit: 2876

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,

Art Unit: 2876

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]).

Art Unit: 2876

**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

Art Unit: 2876

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 vice versa), and therefore an obvious expedient.



Art Unit: 2876

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

Art Unit: 2876

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 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. Regarding claim 6, Margalit teaches a processor module comprises a dual interface chip (i.e., a USB

Art Unit: 2876

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

Art Unit: 2876

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 been 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

Art Unit: 2876

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.

Art Unit: 2876

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.

Art Unit: 2876

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 <b>PTO/SB/08a &amp; PTO/SB/08b</b> <b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>	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 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
W	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  <b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>	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 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	Extron 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  <b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>	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 <del>g</del>
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	<i>Dallas Semiconductor DS9490-DS9490R USB to 1-Wire/iButton Adaptor</i> , Maxim I-C, Sunnyvale CA.	T
	5	HARA, YOSHIKO, <i>Matsushita blends FERAM technology with smart cards</i> , October 1, 2004, CMP Media, Manhasset NY.	T
	6	<i>Japan's Matsushita developing memory cards with smart chip function</i> , October 1, 2004, Mercury News, San Jose CA.	T
	7	<i>OTi-6828 Flash Disk Controller</i> , Ours Technology Inc., Taiwan.	T
	8	<i>Panasonic Develops RFID smartSD Card</i> , October 4, 2004, Palminfocenter.com, Sunnyvale CA.	T
	9	<i>Panasonic Develops Industry's First SD Memory Card with Contactless Smart Card Capabilities</i> , October 1, 2004, The Japan Corporate News Network, Tokyo.	T
	10	ROJAS, PETER, <i>Panasonic's Smart SD adds RFID to the mix</i> , October 4, 2004, Engadget LLC, New York NY.	T
	11	<i>Delivering ultimate security, high performance and ultra low power consumption, SmartMX is now in volume supply</i> , November 18-20, 2003, Cartes 2003, aris Nort Villepinte, France	T
	12	BALABAN, DAN, <i>Digital Rights pits SIMS against Flash Cards</i> , <i>Card Technology</i> , November 2004, pp 24-30, Card Technology, Chicago IL.	T
	13	<i>P5CT072 Secure Dual Interface PKI Smart Card Controller, Rev. 1.3</i> , October 2004, Koninklijke Philips Electronics, The Netherlands	T
	14	<i>Vodafone KK Develops Contactless Smart Card Mobile Handset</i> , May 6, 2004, HiTEK Magazine, Dubai	T
	15	<i>SmartSD Card Structure</i>	T

  
 Examiner Signature

1/17/06  
 Date Considered

<b>Notice of References Cited</b>	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

**Examiner**

Uyen-Chau N. Le

**Applicant(s)/Patent under Reexamination**

RYAN ET AL.

**Art Unit**

2876

√	Rejected
=	Allowed

-	(Through numeral) Cancelled
+	Restricted

N	Non-Elected
I	Interference

A	Appeal
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**



<b>Application/Control No.</b> 10/990,296	<b>Applicant(s)/Patent under Reexamination</b> RYAN ET AL.	
<b>Examiner</b> Uyen-Chau N. Le	<b>Art Unit</b> 2876	

SEARCHED			
Class	Subclass	Date	Examiner
SEARCH	UPDATED	1/17/2006	UCL

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

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner



UNITED STATES PATENT AND TRADEMARK OFFICE

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

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  
CLEVELAND 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.

A

<b>Interview Summary</b>	Application No. 10/990,296	Applicant(s) RYAN ET AL.	
	Examiner Uyen-Chau N. Le	Art Unit 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.



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: L.c, Uyen Chau N.  
phone: 571-272-2397

Art Unit: 2876

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 supersedes 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 802.11 802.11 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~~ 802.11 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; 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.

**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 appliance 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~~ 802.11 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 a Bluetooth /WLAN ~~812.11~~ 802.11 compatible 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 releasably 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 consisting 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 require 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 LAN. 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 802.11~~ 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 capabilities 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 between 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 requirements, 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:

Functionally, 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 802.11, 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 claim 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,



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

<b>Application Number:</b>	10990296
<b>Filing Date:</b>	16-Nov-2004
<b>Title of Invention:</b>	Multi-interface compact personal token apparatus and methods of use
<b>First Named Inventor:</b>	Dennis J. Ryan
<b>Filer:</b>	Dwight A. Stauffer
<b>Attorney Docket Number:</b>	Ryan C-4

Filed as Small Entity

### Utility Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Basic Filing:</b>				
<b>Pages:</b>				
<b>Claims:</b>				
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:

IPR2022-00412

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Extension-of-Time:</b>				
<b>Miscellaneous:</b>				
Request for continued examination	2801	1	395	395
<b>Total in USD (\$)</b>				<b>645</b>

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	1031229
<b>Application Number:</b>	10990296
<b>Confirmation Number:</b>	2050
<b>Title of Invention:</b>	Multi-interface compact personal token apparatus and methods of use
<b>First Named Inventor:</b>	Dennis J. Ryan
<b>Customer Number:</b>	37053
<b>Filer:</b>	Dwight A. Stauffer
<b>Filer Authorized By:</b>	
<b>Attorney Docket Number:</b>	Ryan C-4
<b>Receipt Date:</b>	25-APR-2006
<b>Filing Date:</b>	16-NOV-2004
<b>Time Stamp:</b>	23:39:14
<b>Application Type:</b>	Utility
<b>International Application Number:</b>	

### 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
-----------------	----------------------	-----------	------------------	------------	-------

IPR2022-00412

1		Ryan_C-4_rce_and_Amend ment 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:**

<b>Total Files Size (in bytes):</b>		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  <b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>	Application Number	<b>10/990,296</b>
	Filing Date	<b>November 16, 2004</b>
	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	
	JJ	US 6,342,839	01-29-2002	Curkendall et al.	

\_\_\_\_\_  
Examiner Signature

\_\_\_\_\_  
Date Considered



substitute forms PTO/SB/08a & PTO/SB/08b  <b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>	Application Number	<b>10/990,296</b>
	Filing Date	<b>November 16, 2004</b>
	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	<i>ACR38CT Contactless SIM Tracker Technical Specification</i> , Advanced Card Systems Ltd., Hong Kong.	T
	2	<i>ACR38DT Dual Key Technical Specifications, Version 1.3</i> , September 2004, Advanced Card Systems Ltd., Hong Kong.	T

\_\_\_\_\_  
Examiner Signature

\_\_\_\_\_  
Date Considered

substitute forms PTO/SB/08a & PTO/SB/08b  <b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>	Application Number	<b>10/990,296</b>
	Filing Date	<b>November 16, 2004</b>
	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	<i>Dallas Semiconductor DS1490F 2-in-1 Fob</i> , Dallas Semiconductor, Dallas TX.	T
	4	<i>Dallas Semiconductor DS9490R-DS9490B USB to 1-Wire/iButton Adaptor</i> , Maxim I-C, Sunnyvale CA.	T
	5	HARA, YOSHIKO, <i>Matsushita blends FERAM technology with smart cards</i> , EE Times, October 1, 2004, CMP Media, Manhasset NY.	T
	6	<i>Japan's Matsushita developing memory cards with smart chip function</i> , October 1, 2004, Mercury News, San Jose CA.	T
	7	<i>OTi-6828 Flash Disk Controller</i> , Ours Technology Inc., Taiwan.	T
	8	<i>Panasonic Develops RFID smartSD Card</i> , October 4, 2004, Palminfocenter.com, Sunnyvale CA.	T
	9	<i>Panasonic Develops Industry's First SD Memory Card with Contactless Smart Card Capabilities</i> , October 1, 2004, The Japan Corporate News Network, Tokyo.	T
	10	ROJAS, PETER, <i>Panasonic's Smart SD adds RFID to the mix</i> , October 4, 2004, Engadget I.I.C, New York NY.	T
	11	<i>Delivering ultimate security, high performance and ultra low power consumption, SmartMX is now in volume supply</i> , November 18-20, 2003, Cartes 2003, aris Nort Villepinte, France	T
	12	BALABAN, DAN, <i>Digital Rights pits SIMS against Flash Cards, Card Technology</i> , November 2004, pp 24, 25, 26, 28, 30, Card Technology, Chicago IL.	T
	13	<i>Smart MX P5CT072 Secure Dual Interface PKI Smart Card Controller, Rev. 1.3</i> , October 2004, Koninklijke Philips Electronics NV, The Netherlands	T
	14	<i>Vodafone KK Develops Contactless Smart Card Mobile Handset</i> , May 6, 2004, HiTEK Magazine, Dubai	T
	15	<i>SmartSD Card Structure</i> , Panasonic	T

\_\_\_\_\_  
Examiner Signature

\_\_\_\_\_  
Date Considered



19 BUNDESREPUBLIK  
DEUTSCHLAND



DEUTSCHES  
PATENTAMT

12 **Offenlegungsschrift**  
10 **DE 196 31 050 A 1**

51 Int. Cl.°:  
**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

DE 196 31 050 A 1

71 Anmelder:  
Bergler, Frank, 75223 Niefern-Öschelbronn, DE;  
Käuffert, Uwe, 75180 Pforzheim, DE

72 Erfinder:  
gleich Anmelder

56 Entgegenhaltungen:

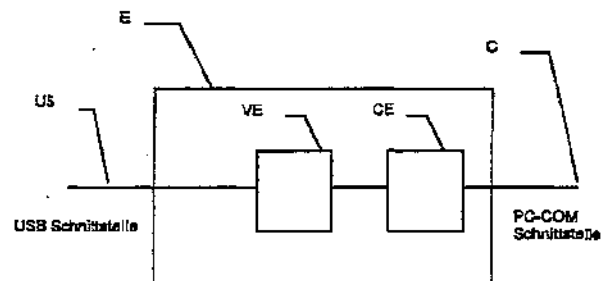
DE 39 31 511 C2  
DE 41 15 242 A1  
DE 33 22 690 A1  
US 50 88 385 A  
EP 0 17 035 A1

STRASS, Hermann: Universell, seriell, aber kein Bus.  
In: Elektronik 20, 1995, S.32-34,38-42;  
LANGER, Klaus, D.: Softwareverarbeitung 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.



DE 196 31 050 A 1

Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

BUNDESDRUCKEREI 12. 97 102062/02 23/27

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.

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. 5

Hierzu 1 Seite(n) Zeichnungen

10

15

20

25

30

35

40

45

50

55

60

65

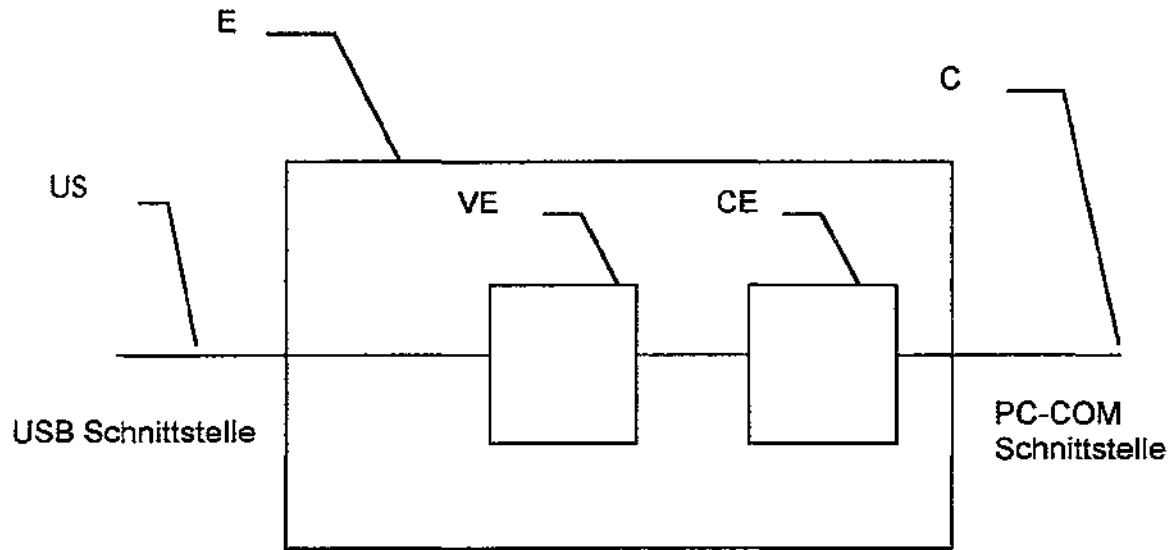


Fig. 1

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 preferred 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 fourth 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.



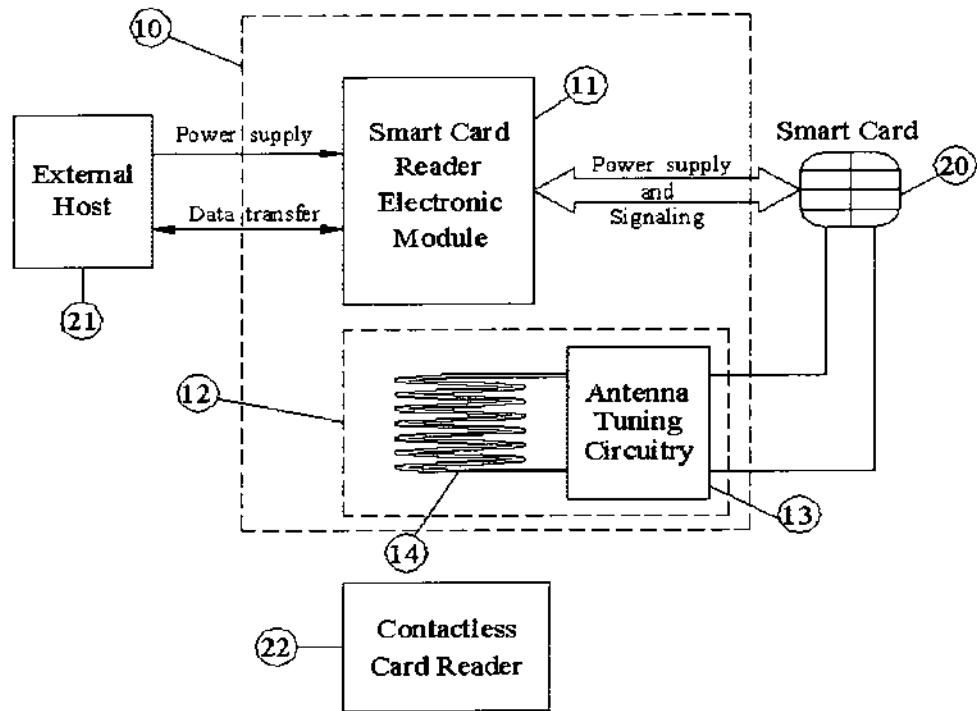


FIG. 1

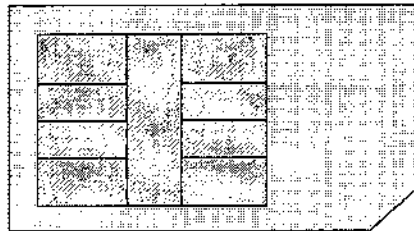


FIG. 2

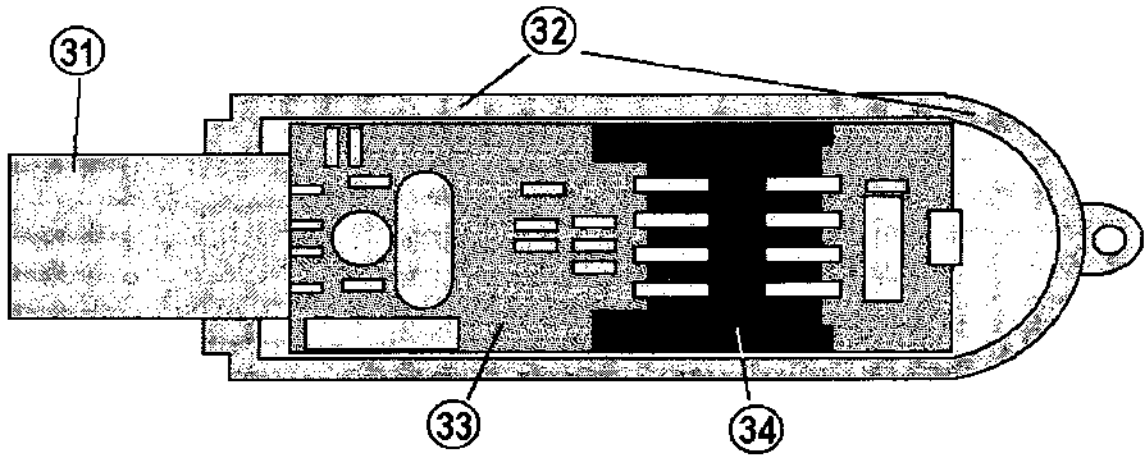


FIG. 3

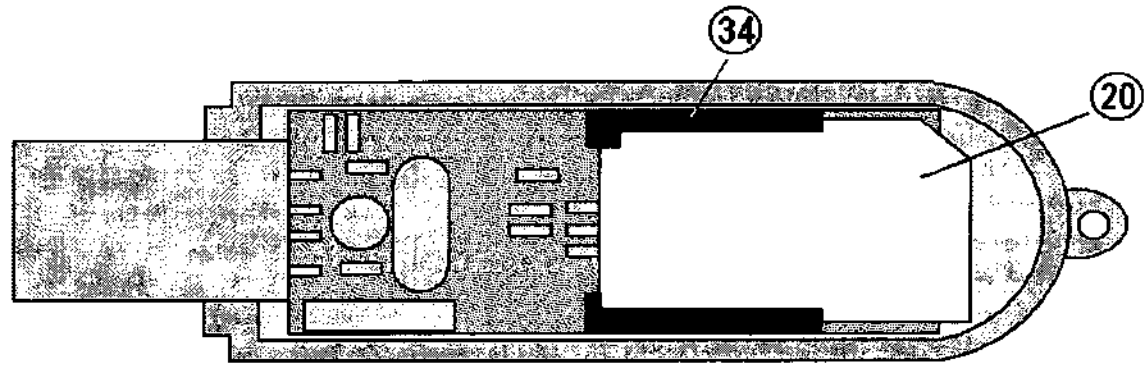


FIG. 4

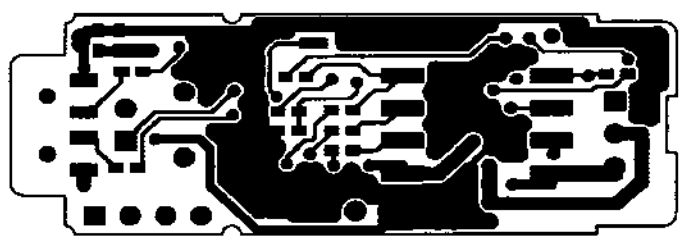


FIG. 5A

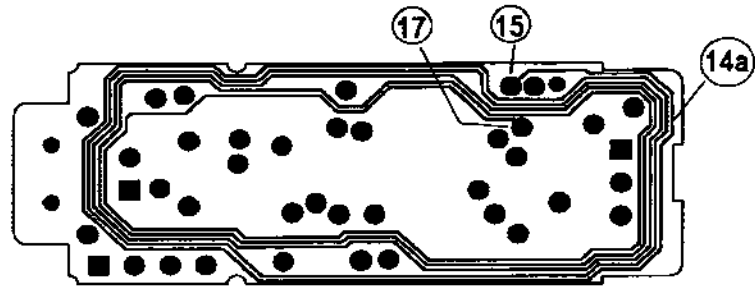


FIG. 5B

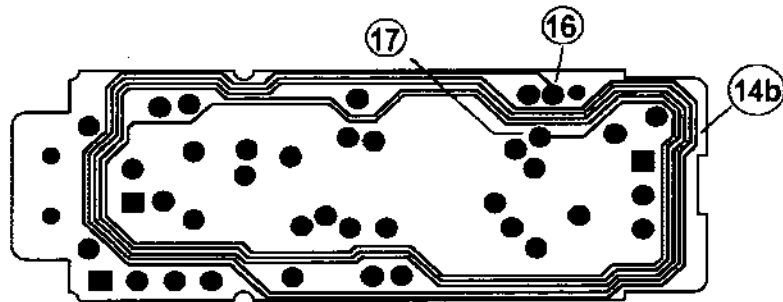


FIG. 5C

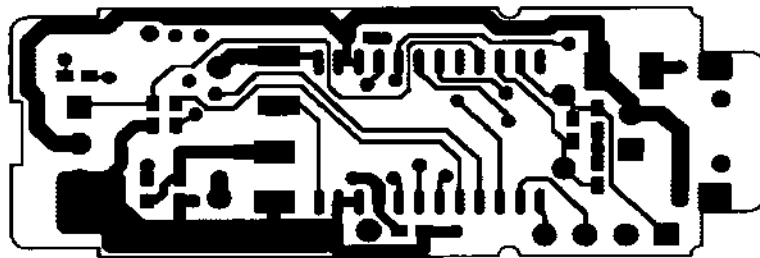


FIG. 5D

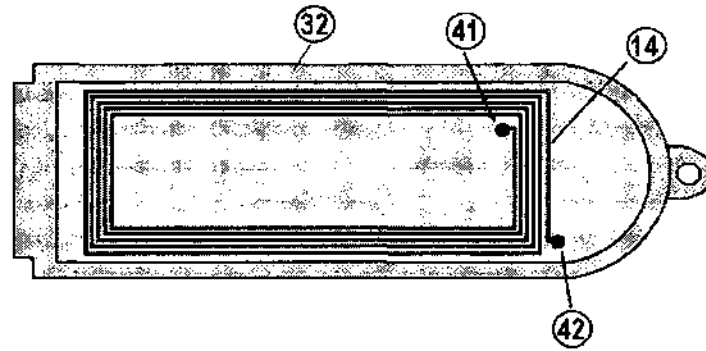


FIG. 6

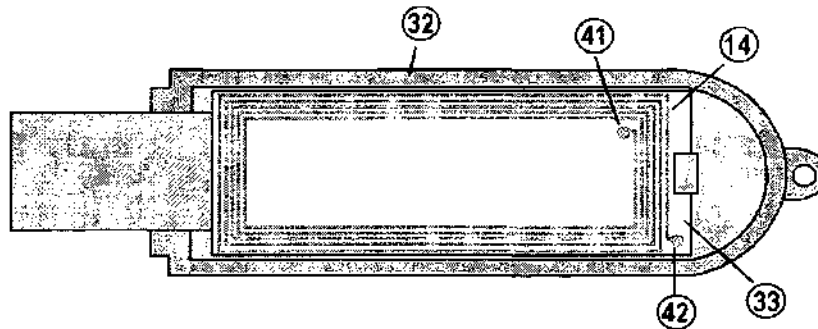


FIG. 7

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 disposed 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.

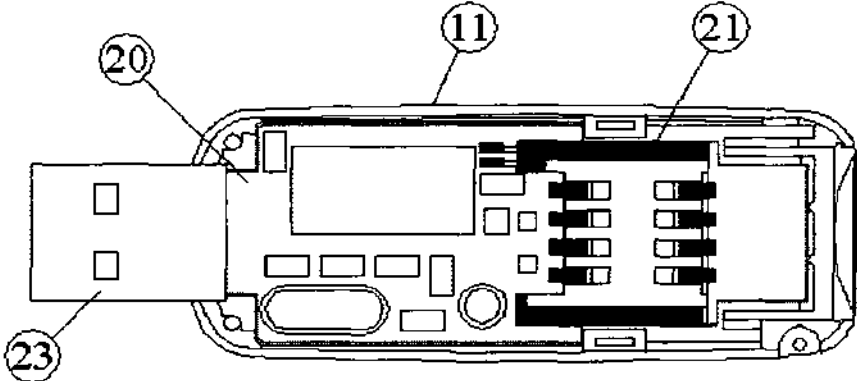


FIG. 1

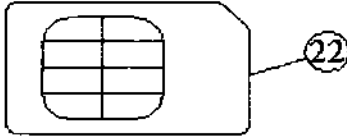


FIG. 2

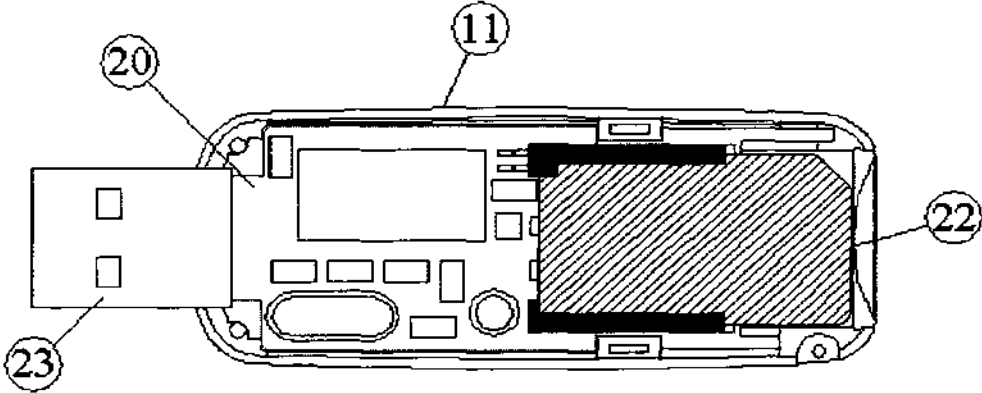


FIG. 3

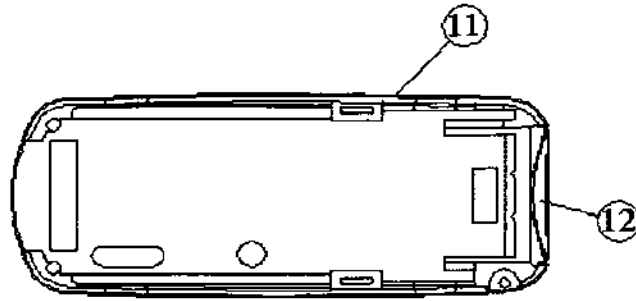


FIG. 4A

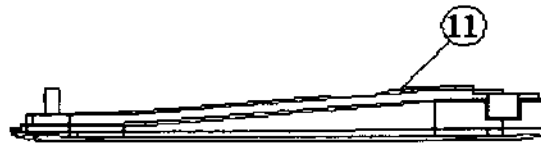


FIG. 4B

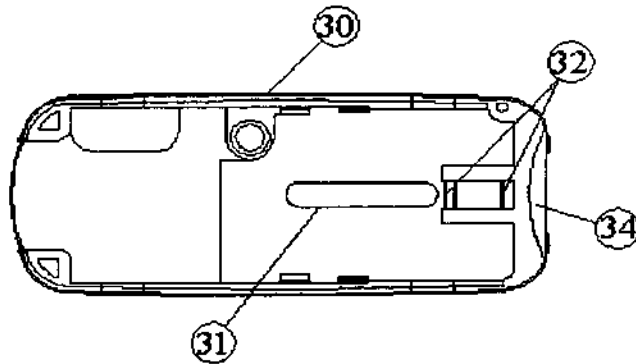


FIG. 5A

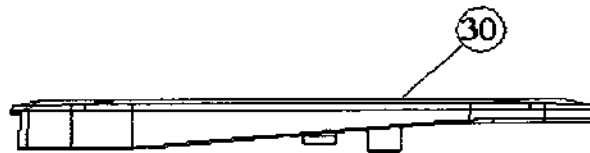


FIG. 5B

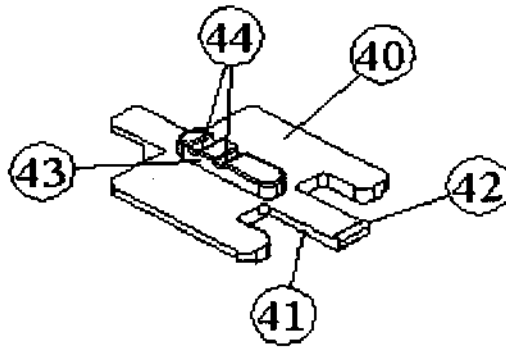


FIG. 6A

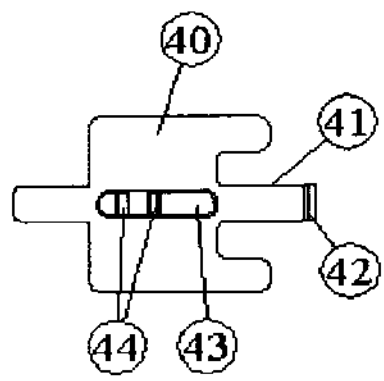


FIG. 6B

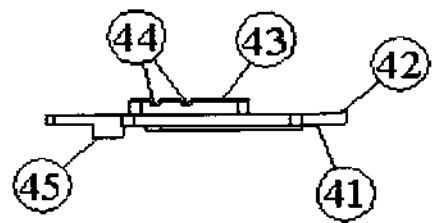


FIG. 6C

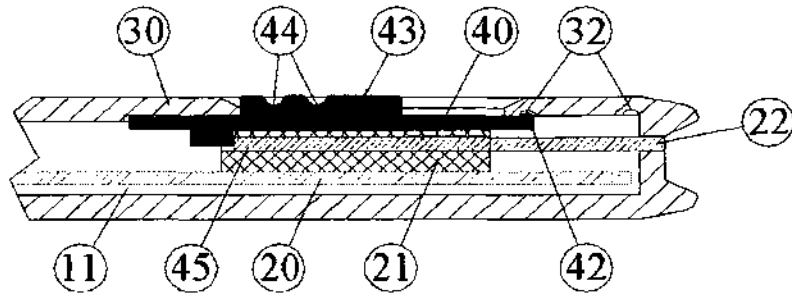


FIG. 7A

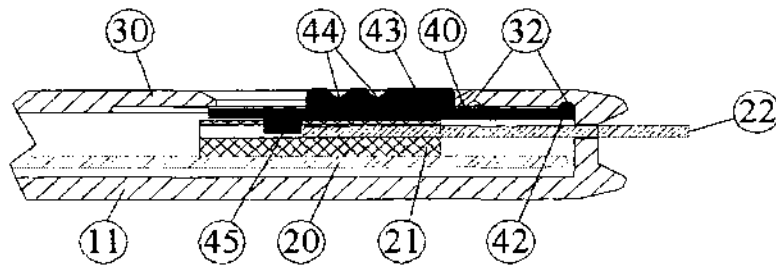


FIG. 7B

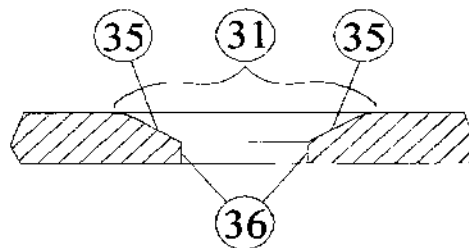


FIG. 8A

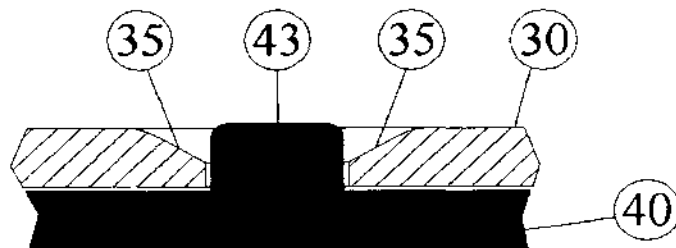


FIG. 8B

(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. <sup>7</sup>	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 O L (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

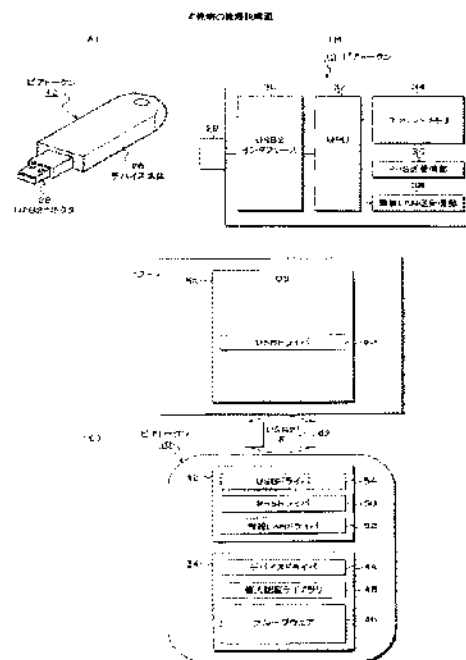
(54) 【発明の名称】 情報処理デバイス、情報処理方法及びプログラム

(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、ヒアツーヒ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・エニウェア」”、[平成15年2月3日検索]、インターネット<URL>： <http://www.beemail.jp/anywhere.html> URL： <http://www.beemail.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MC I A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、メモリスティ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は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USB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よっては、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よっては、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ァラル装置である。

## 【0031】

このピアトークン10は、例えば出張先で使用するこのできるパーソナルコンピュータ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の使用環境にあつては、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認し、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16、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54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し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認して、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認し、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による接続を確認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の処理機能の一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側にあつては、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31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、使用後にあつ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にあつては、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側にあつては、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にあつては、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にあつては、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にあつては、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にあつては、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にあつては、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ます。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ります。

## 【0078】

そこでピアトークン10にあつては、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

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しようとする時、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64に送る。

【0087】

これを受けて携帯電話64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にあつては、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側においては、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におい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若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若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

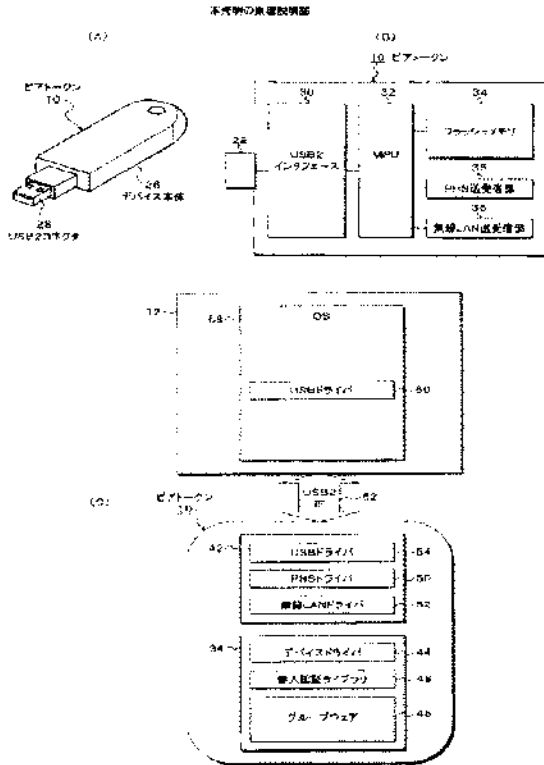
14-1～14-4：ピア装置

15：LAN

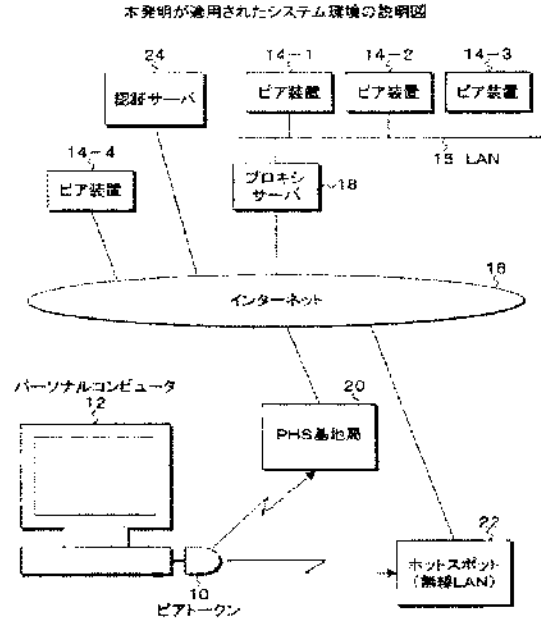
16 : インターネット  
18 : プロキシサーバ  
20 : PHS基地局  
22 : ホットスポット (無線LAN)  
24 : 認証サーバ  
26 : デバイス本体  
28 : USB2コネクタ  
30, 62 : USB2インタフェース  
32 : MPU (プロセッサ)  
34 : フラッシュメモリ (不揮発メモリ)  
36 : PHS送受信部  
38 : 無線LAN送受信部  
40, 68 : メモリマップ  
42 : デバイス処理プログラム (トークンOS)  
44 : デバイスドライバ  
45 : インストール要求画面  
46 : グループウェア  
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】

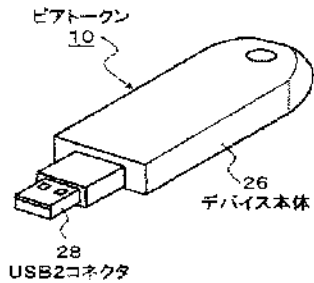


【図2】



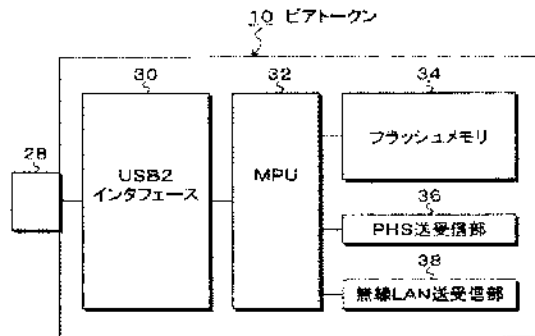
【図3】

本発明によるキー型ピアトークンの外観の説明図



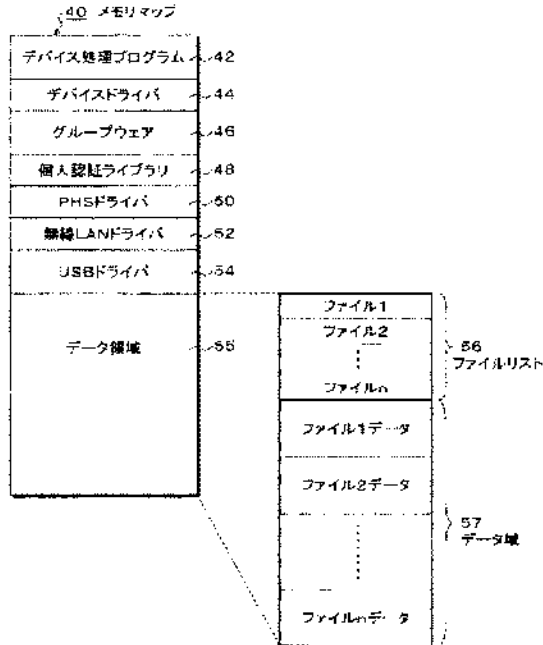
【図4】

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



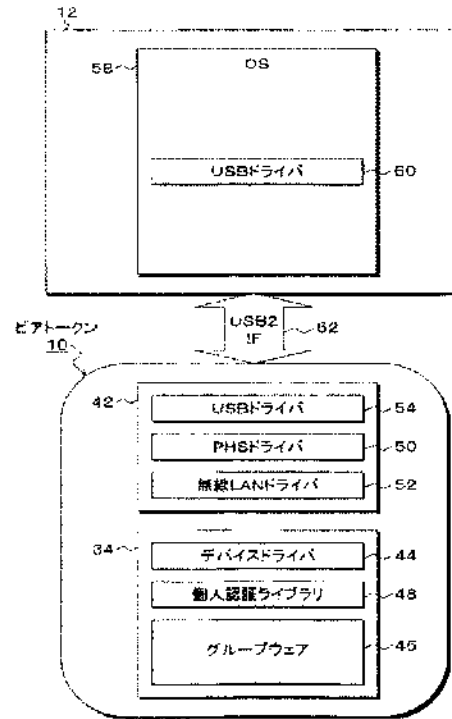
【図5】

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



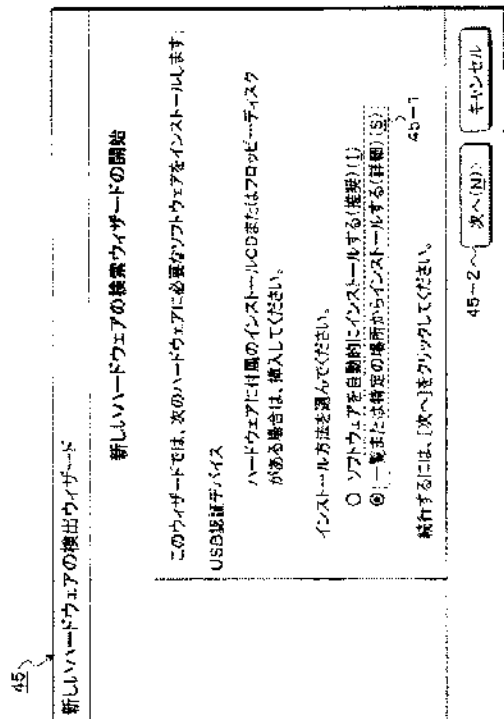
【図6】

本発明のビートル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



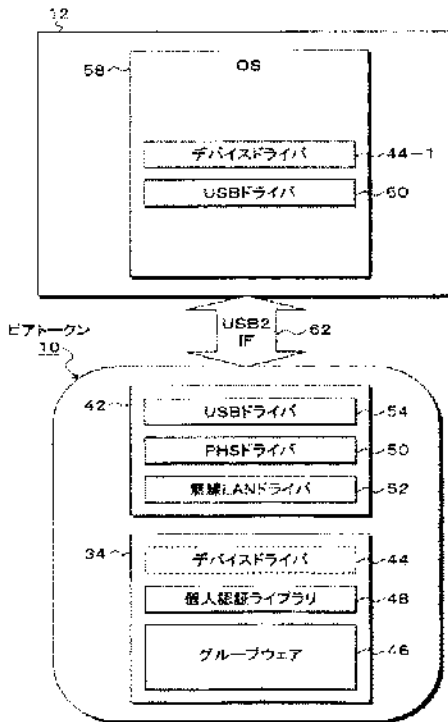
【図7】

ビートル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



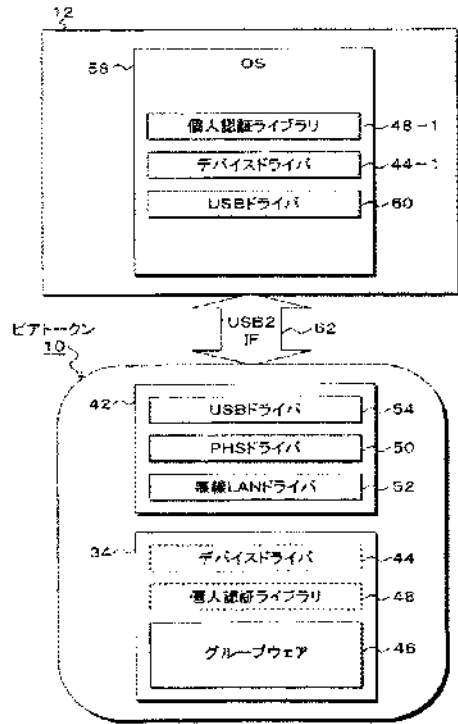
【図8】

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



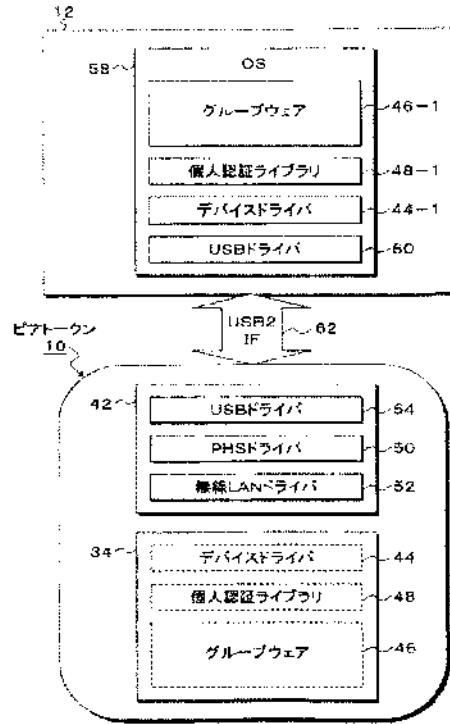
【図9】

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



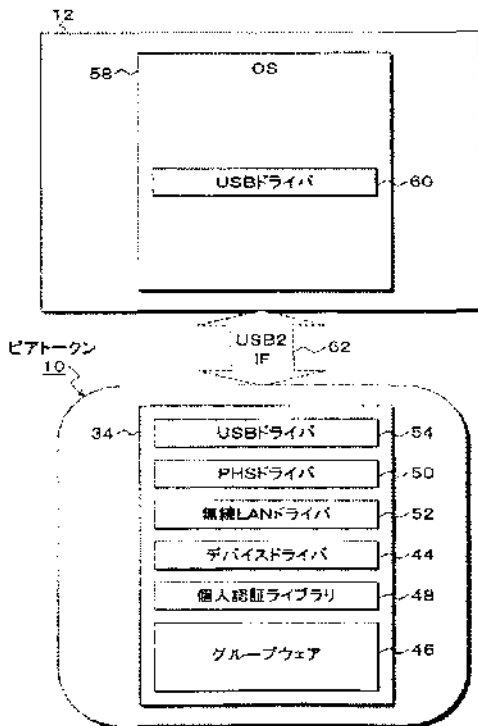
【図10】

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



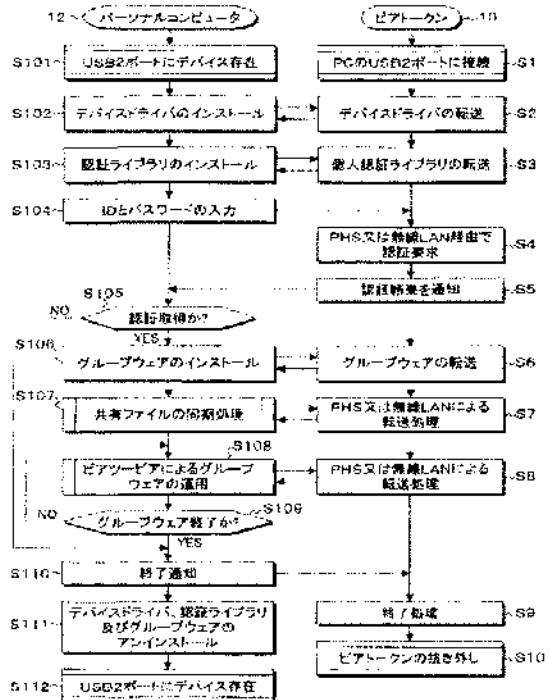
【図11】

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抜き出した際の説明図



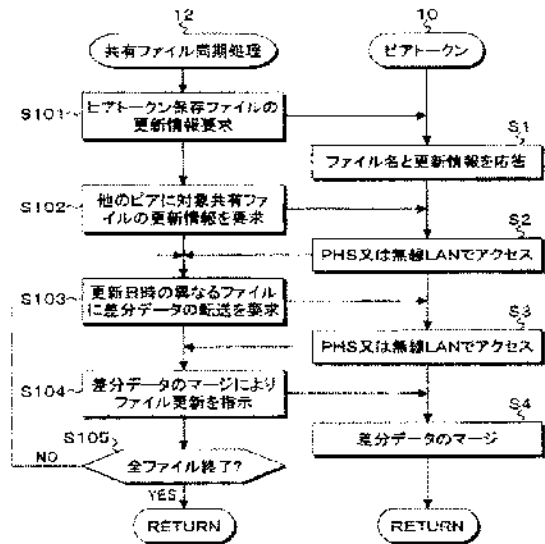
【図12】

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



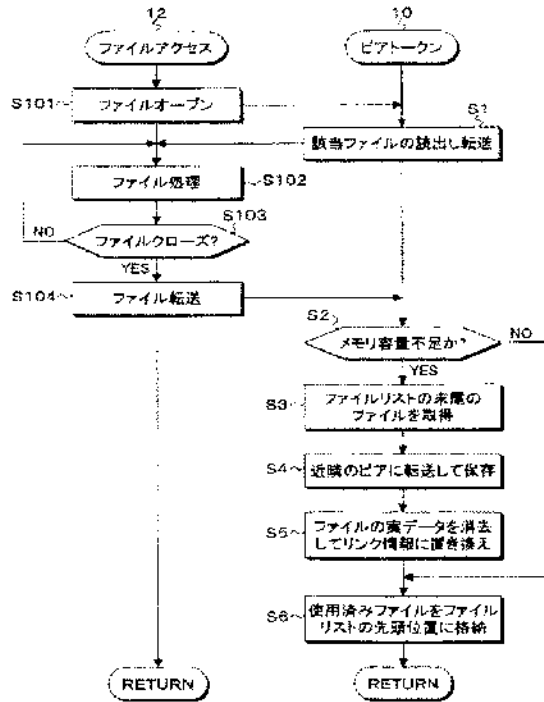
【図13】

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



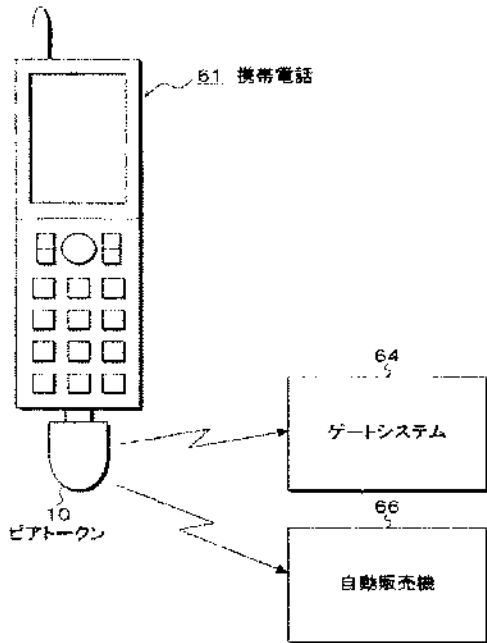
【図14】

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



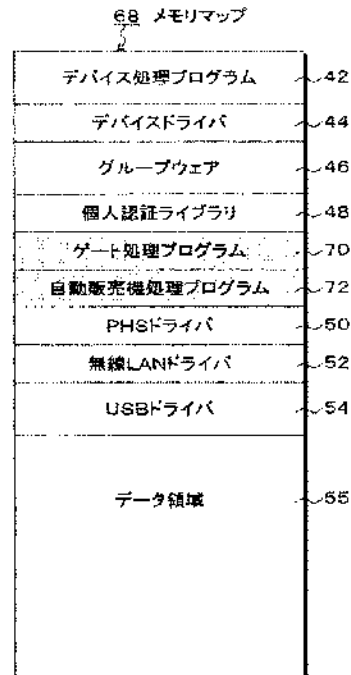
【図15】

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



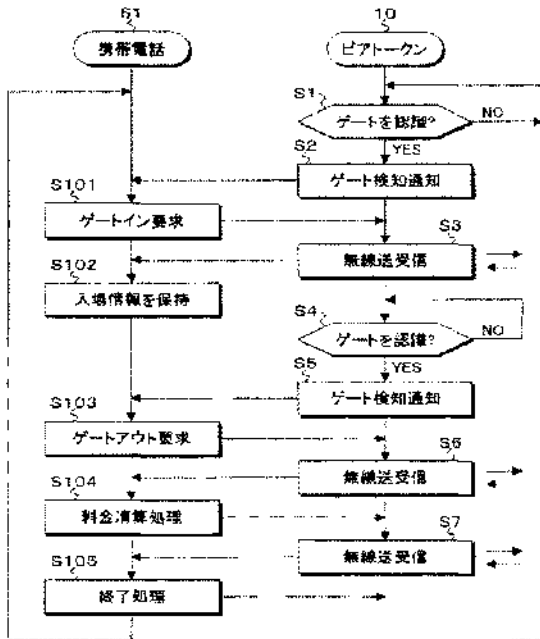
【図16】

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



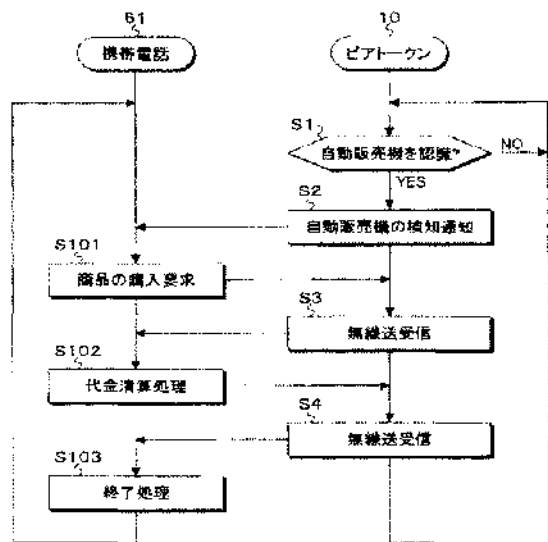
【図17】

ゲートシステムを対象とした本発明のピアトゥー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ゥーンと携帯電話の処理手順のフローチャート



(51)Int.Cl.

F I

テーマコード (参考)

G 0 6 F 9/06 6 6 0 F

F ターム(参考) 5B014 FA14

5B076 AB20 BA05 BA10 BB12 BB18 FB01

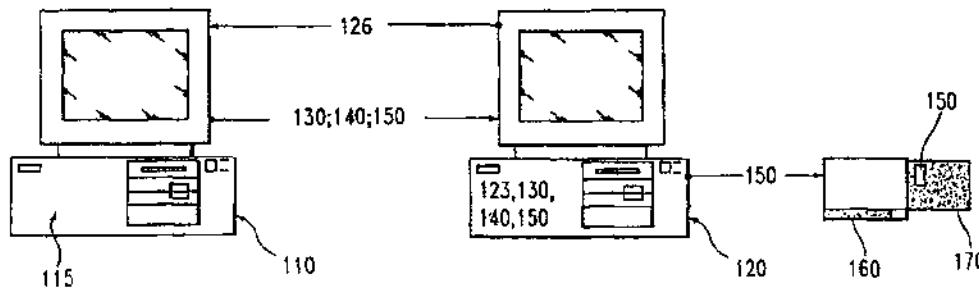
5B085 AA04 AE02 AE12 AE23 BE01 BF04 BG01 BG02 BG07



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification<sup>6</sup> : <b>G06F 17/60, G07F 7/02</b></p>	<p><b>A1</b></p>	<p>(11) International Publication Number: <b>WO 99/52051</b> (43) International Publication Date: 14 October 1999 (14.10.99)</p>
<p>(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 3AL (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).</p>		<p>(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).  <b>Published</b> <i>With international search report.</i></p>

(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.

<b>AL</b>	Albania	<b>ES</b>	Spain	<b>LS</b>	Lesotho	<b>SI</b>	Slovenia
<b>AM</b>	Armenia	<b>FI</b>	Finland	<b>LT</b>	Lithuania	<b>SK</b>	Slovakia
<b>AT</b>	Austria	<b>FR</b>	France	<b>LU</b>	Luxembourg	<b>SN</b>	Senegal
<b>AU</b>	Australia	<b>GA</b>	Gabon	<b>LV</b>	Latvia	<b>SZ</b>	Swaziland
<b>AZ</b>	Azerbaijan	<b>GB</b>	United Kingdom	<b>MC</b>	Monaco	<b>TD</b>	Chad
<b>BA</b>	Bosnia and Herzegovina	<b>GE</b>	Georgia	<b>MD</b>	Republic of Moldova	<b>TG</b>	Togo
<b>BB</b>	Barbados	<b>GH</b>	Ghana	<b>MG</b>	Madagascar	<b>TJ</b>	Tajikistan
<b>BE</b>	Belgium	<b>GN</b>	Guinea	<b>MK</b>	The former Yugoslav Republic of Macedonia	<b>TM</b>	Turkmenistan
<b>BF</b>	Burkina Faso	<b>GR</b>	Greece	<b>ML</b>	Mali	<b>TR</b>	Turkey
<b>BG</b>	Bulgaria	<b>HU</b>	Hungary	<b>MN</b>	Mongolia	<b>TT</b>	Trinidad and Tobago
<b>BJ</b>	Benin	<b>IE</b>	Ireland	<b>MR</b>	Mauritania	<b>UA</b>	Ukraine
<b>BR</b>	Brazil	<b>IL</b>	Israel	<b>MW</b>	Malawi	<b>UG</b>	Uganda
<b>BY</b>	Belarus	<b>IS</b>	Iceland	<b>MX</b>	Mexico	<b>US</b>	United States of America
<b>CA</b>	Canada	<b>IT</b>	Italy	<b>NE</b>	Niger	<b>UZ</b>	Uzbekistan
<b>CF</b>	Central African Republic	<b>JP</b>	Japan	<b>NL</b>	Netherlands	<b>VN</b>	Viet Nam
<b>CG</b>	Congo	<b>KE</b>	Kenya	<b>NO</b>	Norway	<b>YU</b>	Yugoslavia
<b>CH</b>	Switzerland	<b>KG</b>	Kyrgyzstan	<b>NZ</b>	New Zealand	<b>ZW</b>	Zimbabwe
<b>CI</b>	Côte d'Ivoire	<b>KP</b>	Democratic People's Republic of Korea	<b>PL</b>	Poland		
<b>CM</b>	Cameroon	<b>KR</b>	Republic of Korea	<b>PT</b>	Portugal		
<b>CN</b>	China	<b>KZ</b>	Kazakstan	<b>RO</b>	Romania		
<b>CU</b>	Cuba	<b>LC</b>	Saint Lucia	<b>RU</b>	Russian Federation		
<b>CZ</b>	Czech Republic	<b>LJ</b>	Liechtenstein	<b>SD</b>	Sudan		
<b>DE</b>	Germany	<b>LK</b>	Sri Lanka	<b>SE</b>	Sweden		
<b>DK</b>	Denmark	<b>LR</b>	Liberia	<b>SG</b>	Singapore		
<b>EE</b>	Estonia						



**AUTHENTICATED ELECTRONIC COUPON ISSUING AND REDEMPTION**

The present invention relates to an electronic advertisement and coupon issuance and redemption.

5

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.

10

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.

15

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.

20

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.

25

30

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.

35

40

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

45

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  
5 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  
10 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  
15 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  
20 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  
25 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  
35 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  
40 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  
45 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.

5

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 software 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

45

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.

5           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  
10           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  
15           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  
20           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-  
25           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,  
30           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.

35           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  
40           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  
45           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.

5

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

45



computer validates the electronic signatures on the coupons. In step 740, the clearing house reimburses the merchant for the valid coupons.

5 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, 10 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 15 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 20 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:

5

at least one issuing station for generating and transmitting electronic advertisements and electronic coupons according to predetermined criteria;

10

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;

15

at least one smart card for holding information including said electronic coupons;

20

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

25

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.

30

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.

35

3. A system as claimed in claim 2, wherein said user interface program comprises a Web browser running on the customer station.

40

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.

45

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:

5

at least one redemption station; and

at least one smart card reader/writer linked to said redemption station;

10

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.

15

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.

20

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.

25

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.

30

11. A method for advertising and issuing at least one coupon electronically, said method comprising:

35

receiving a request for said electronic coupon from a consumer;

generating at least one electronic advertisement and said electronic coupon;

40

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

45

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.

5 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:

10

reading a list of said electronic coupon stored in said smart card;

deleting from said smart card said electronic coupon which have expired;

15

matching valid said electronic coupon with purchased items; and

extracting valid matching said electronic coupon,

20

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.

25

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;

30

validating said electronic coupon; and

reimbursing a merchant for valid said electronic coupon,

35

whereby said issuing station periodically reimburses merchants collecting said electronic coupon.

40

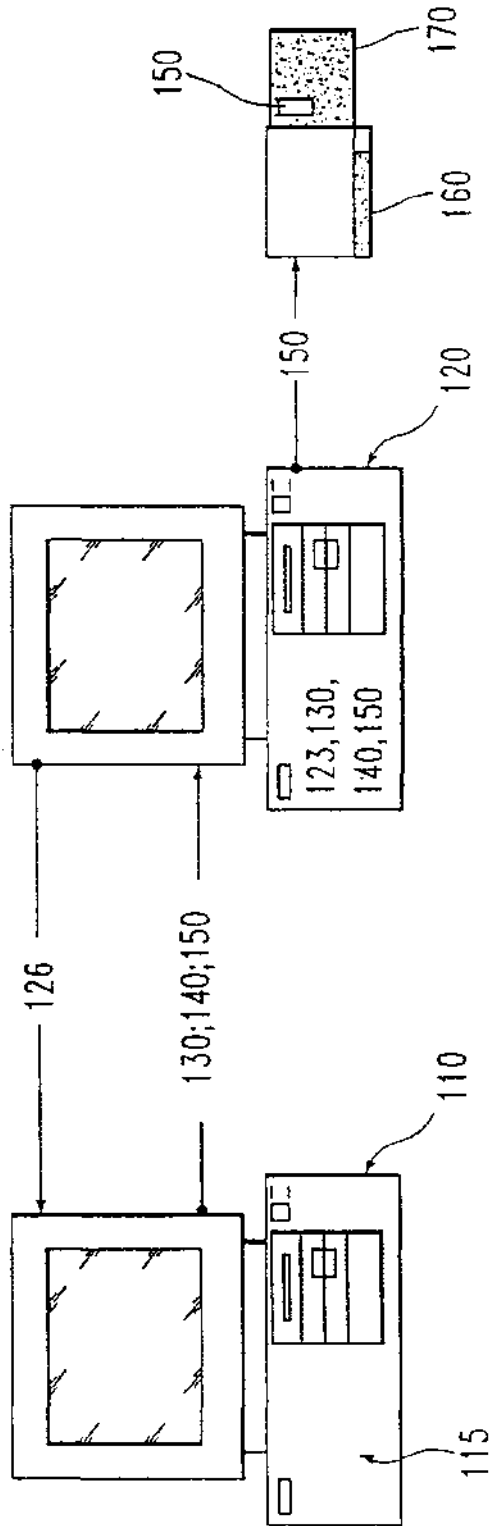


FIG. 1

2/9

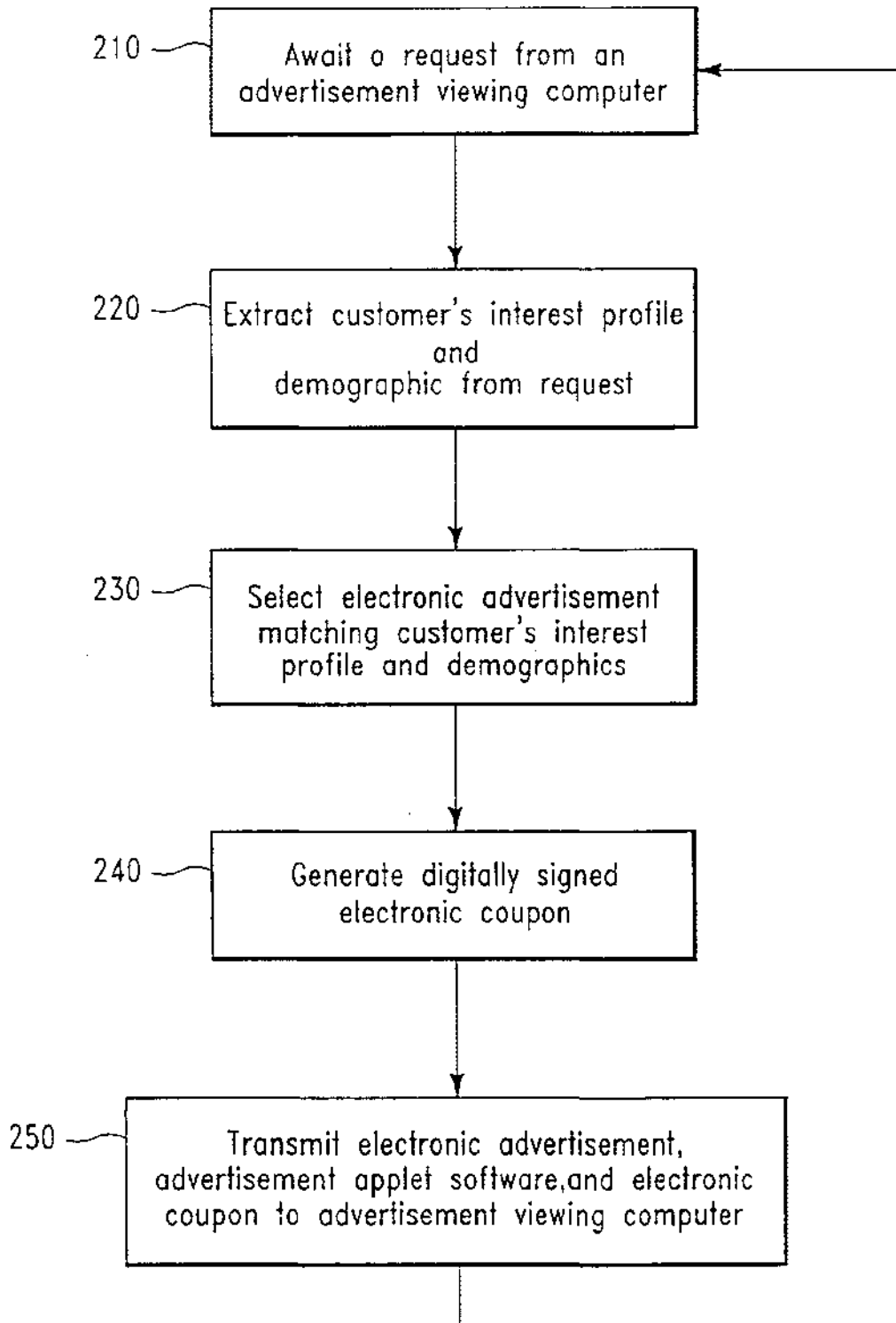


FIG. 2

3/9

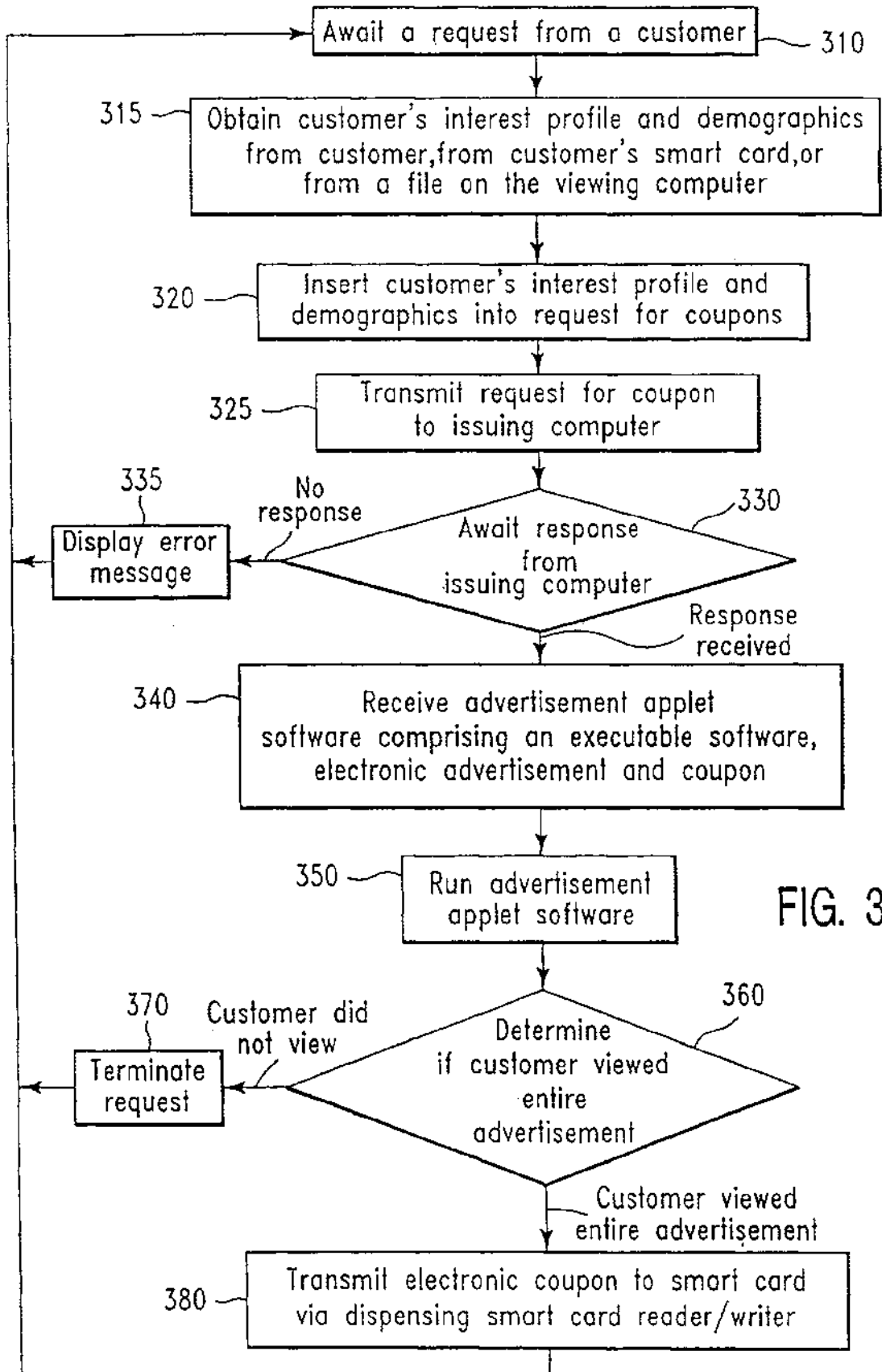


FIG. 3

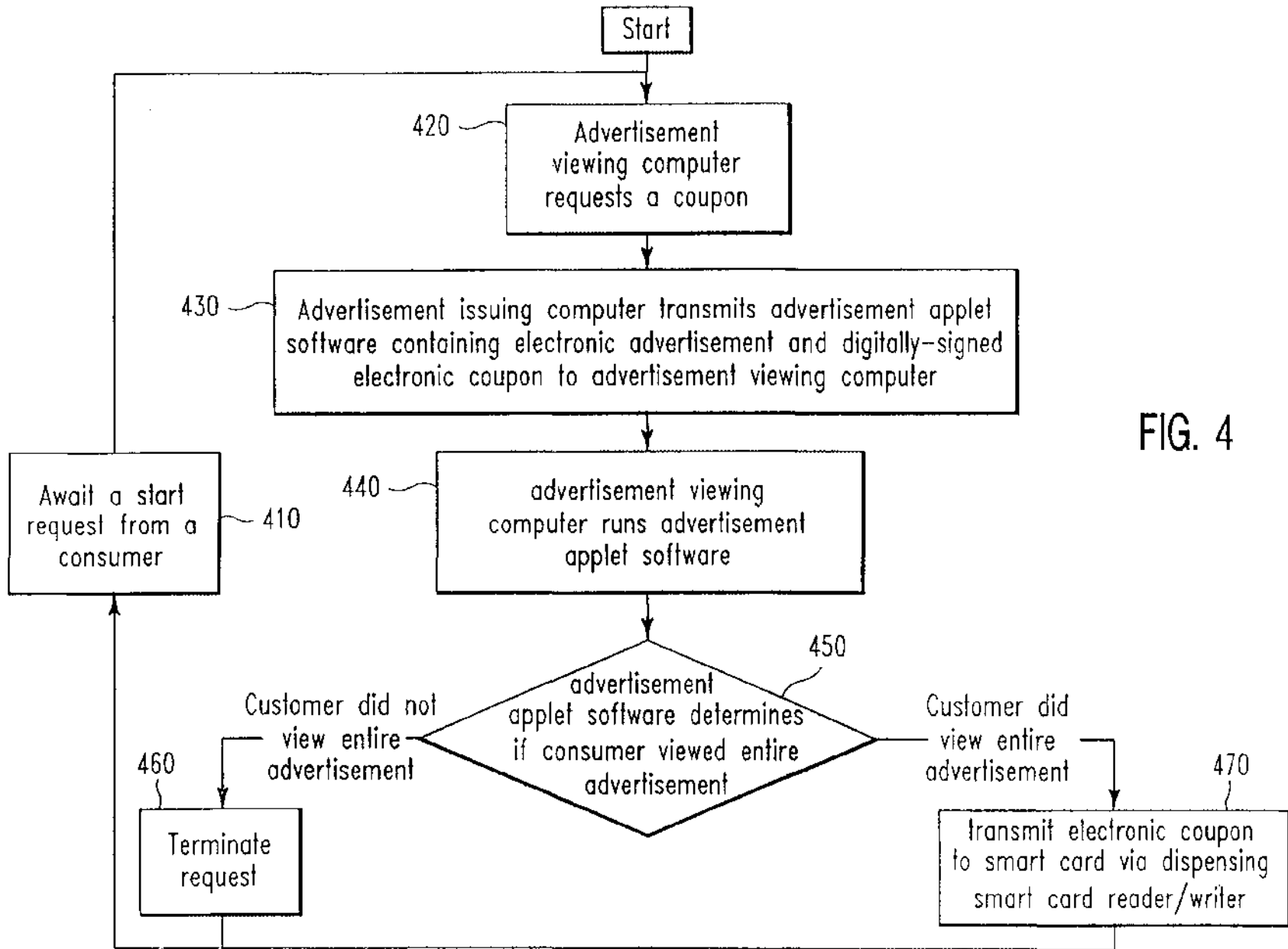


FIG. 4

6/7



5/9

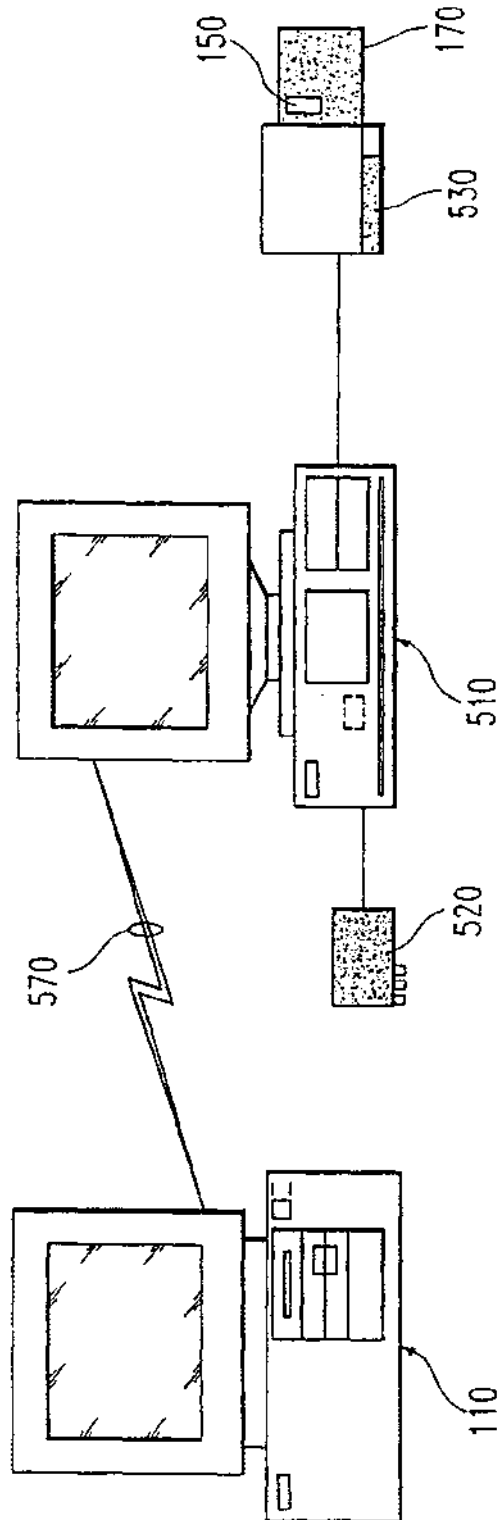


FIG. 5

6/9

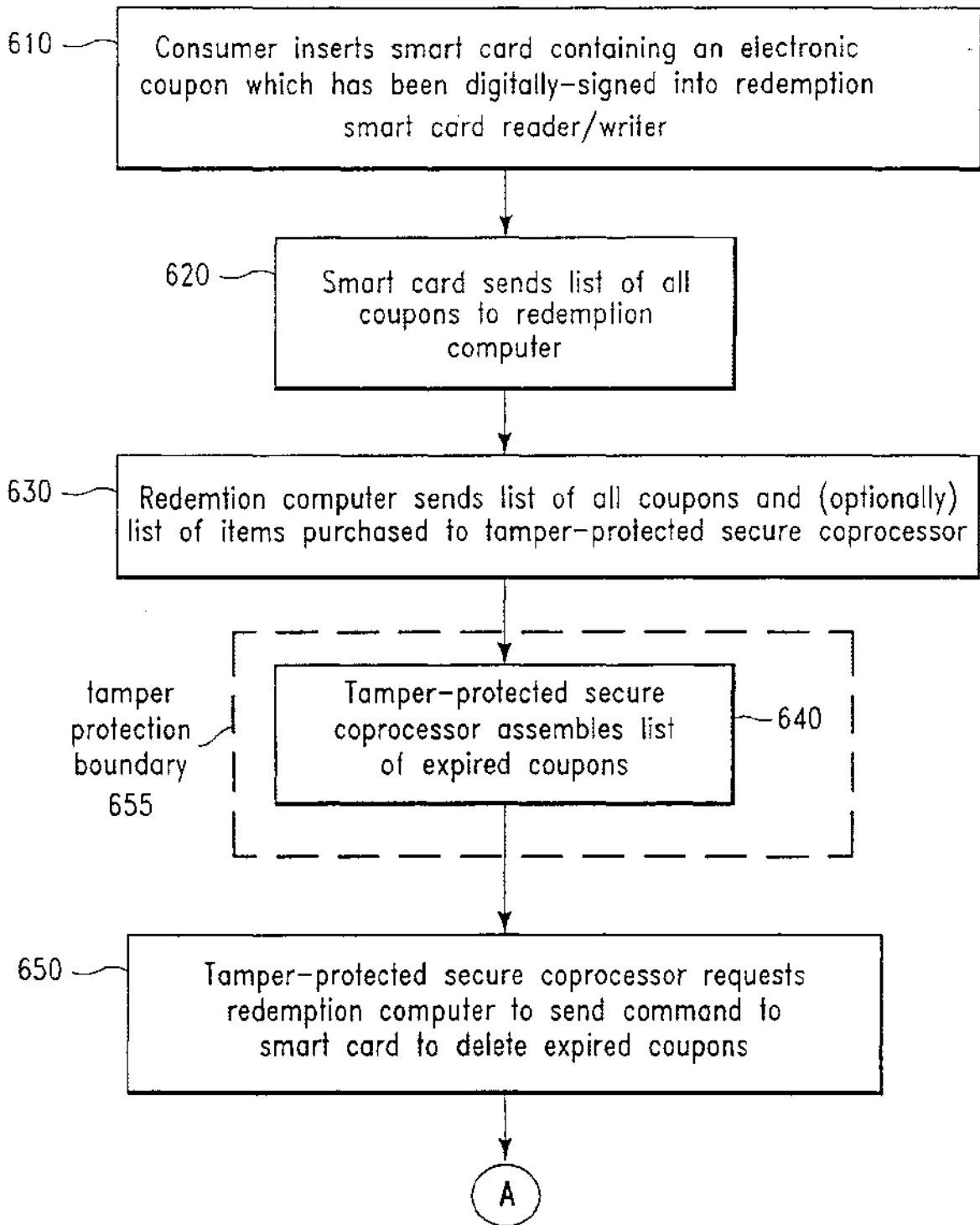
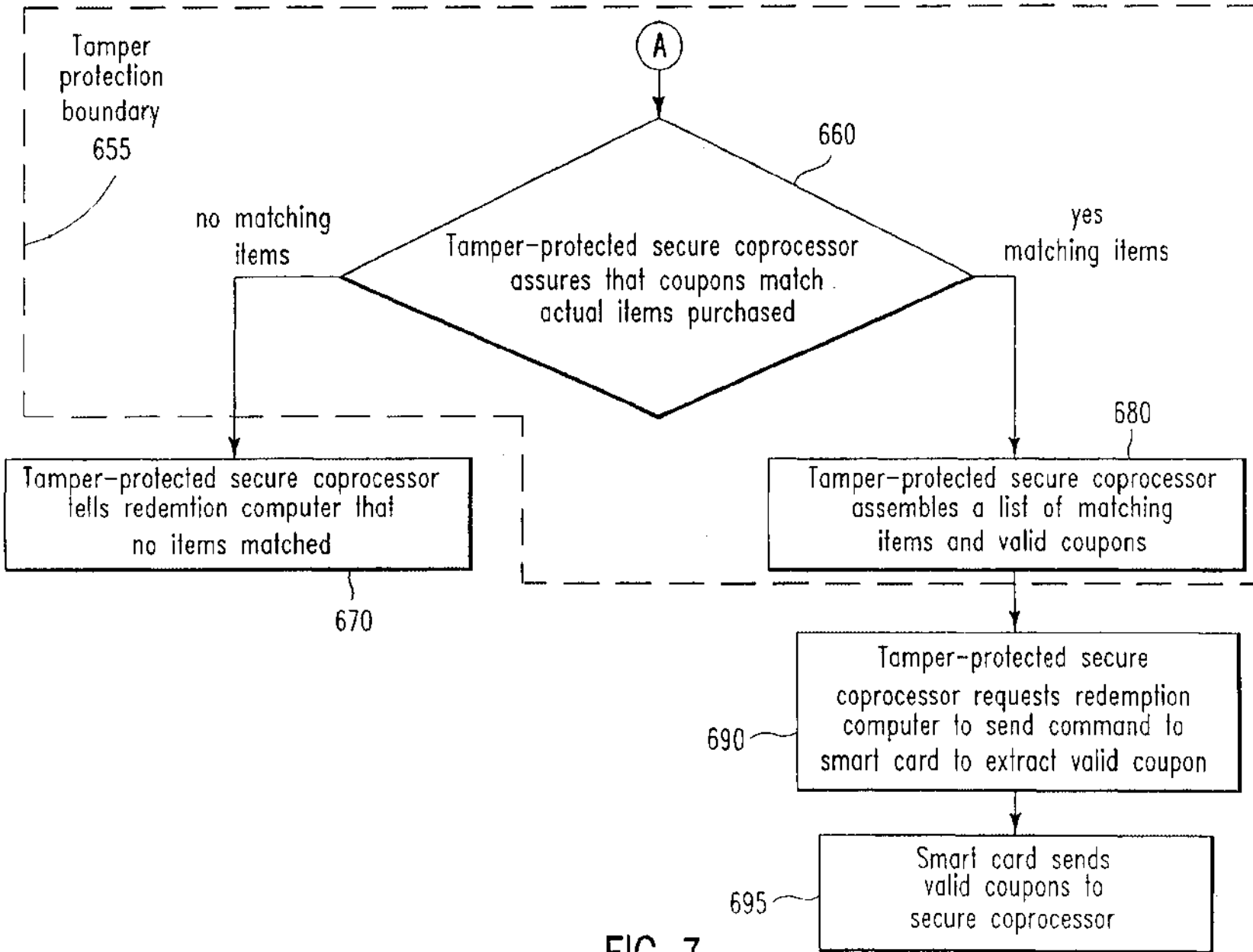


FIG. 6



7/9

FIG. 7

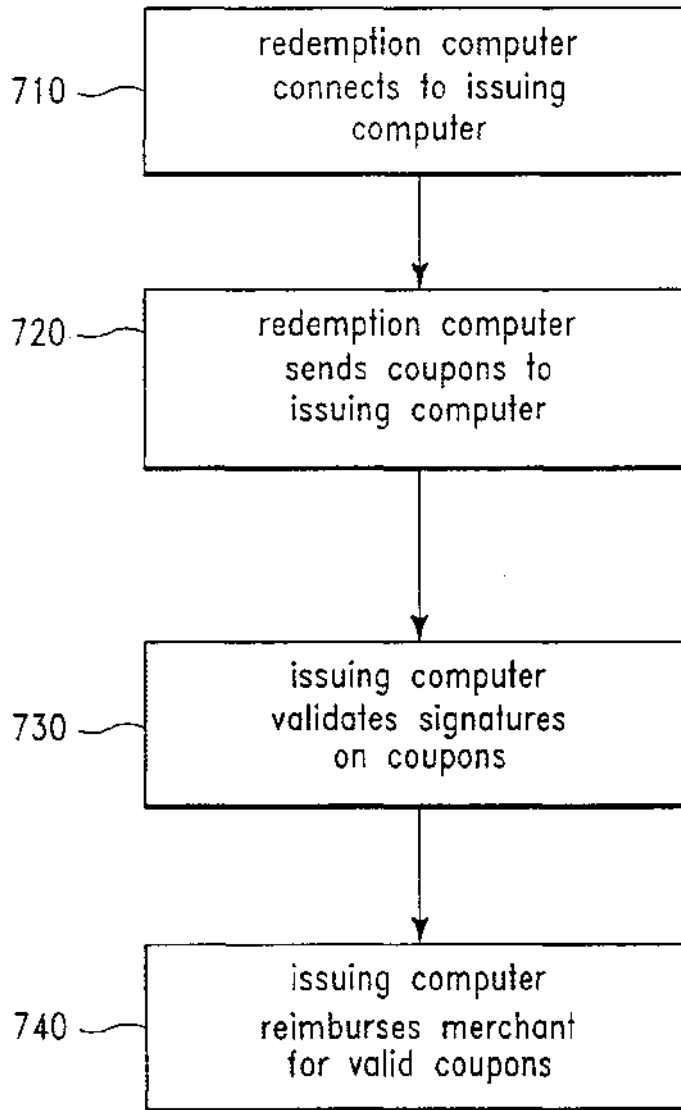


FIG. 8

9/9

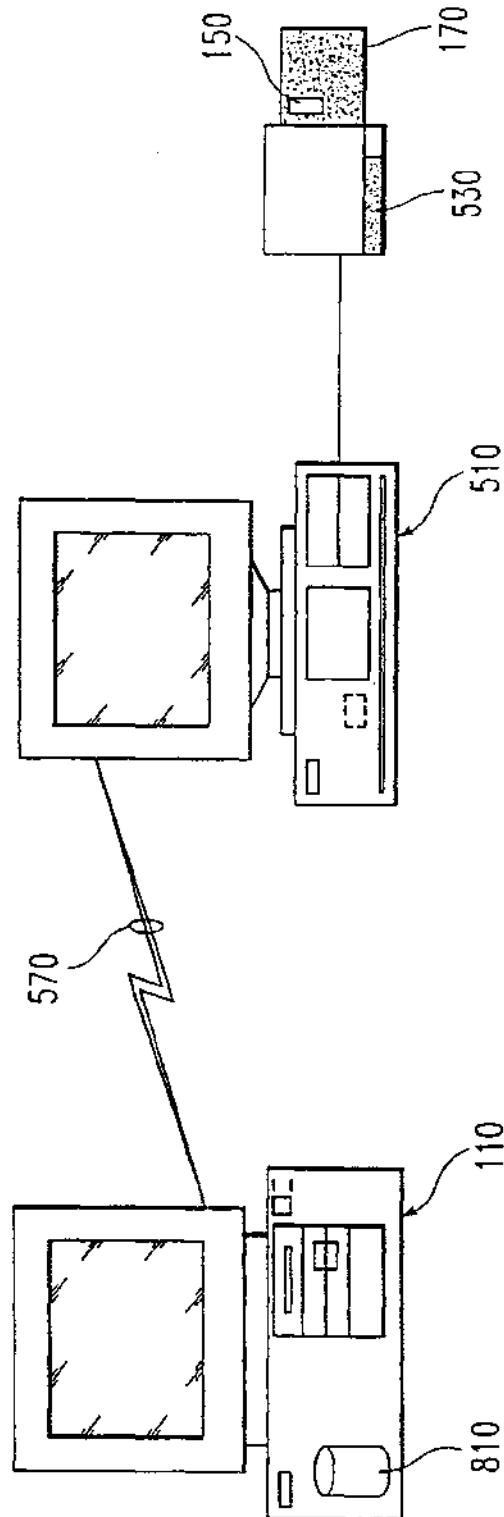


FIG. 9

# INTERNATIONAL SEARCH REPORT

International 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 A A	<p>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 ---</p> <p>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 ---</p> <p>US 5 557 721 A (FITE KENNETH R ET AL) 17 September 1996 ---</p> <p style="text-align: center;">-/--</p>	<p>1-3 7,11,12 1,2,7</p>

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

# INTERNATIONAL SEARCH REPORT

International 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 -----	

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International 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)



<b>(51) Internationale Patentklassifikation <sup>6</sup> :</b> <b>G06F 1/00</b>	<b>A1</b>	<b>(11) Internationale Veröffentlichungsnummer: WO 99/38062</b>  <b>(43) Internationales Veröffentlichungsdatum:</b> 29. Juli 1999 (29.07.99)
<b>(21) Internationales Aktenzeichen:</b> PCT/EP99/00250 <b>(22) Internationales Anmeldedatum:</b> 18. Januar 1999 (18.01.99)	<b>(81) Bestimmungsstaaten:</b> europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).	
<b>(30) Prioritätsdaten:</b> 198 02 316.2            22. Januar 1998 (22.01.98)    DE 198 41 886.8            11. September 1998 (11.09.98)    DE	<b>Veröffentlicht</b> <i>Mit internationalem Recherchenbericht.          Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.</i>	
<b>(71) Anmelder:</b> KOBIL COMPUTER GMBH [DE/DE]; Weinsheimer Strasse 71, D-67547 Worms (DE). <b>(72) Erfinder:</b> ISMET, Koyun; Weinsheimer Strasse 71, D-67547 Worms (DE). <b>(74) Anwalt:</b> REBLE, KLOSE & SCHMITT; Patente + Marken, Postfach 12 15 19, D-68066 Mannheim (DE).		

**(54) Title:** METHOD AND DEVICE FOR CREATING PASSWORDS

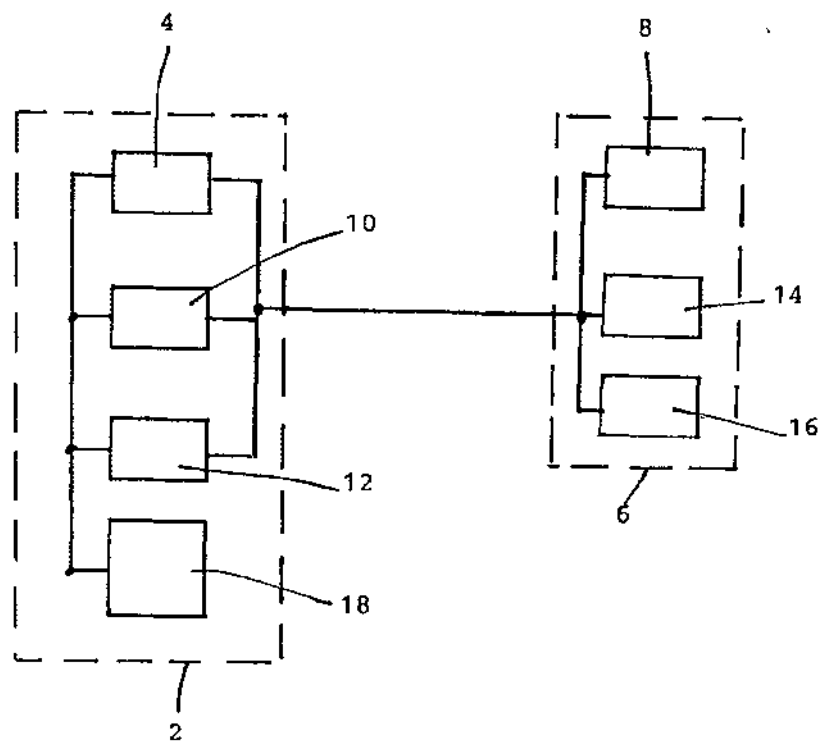
**(54) Bezeichnung:** VERFAHREN UND VORRICHTUNG ZUR ERZEUGUNG VON PASSWÖRTERN

**(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 Republik Mazedonien	TM	Turkmenistan
BF	Burkina Faso	GR	Griechenland	ML	Mali	TR	Türkei
BG	Bulgarien	HU	Ungarn	MN	Mongolei	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MR	Mauretanien	UA	Ukraine
BR	Brasilien	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Island	MX	Mexiko	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	NE	Niger	UZ	Usbekistan
CF	Zentralafrikanische Republik	JP	Japan	NL	Niederlande	VN	Vietnam
CG	Kongo	KE	Kenia	NO	Norwegen	YU	Jugoslawien
CH	Schweiz	KG	Kirgisistan	NZ	Neuseeland	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	PL	Polen		
CM	Kamerun	KR	Republik Korea	PT	Portugal		
CN	China	KZ	Kasachstan	RO	Rumänien		
CU	Kuba	LC	St. Lucia	RU	Russische Föderation		
CZ	Tschechische Republik	LI	Liechtenstein	SD	Sudan		
DE	Deutschland	LK	Sri Lanka	SE	Schweden		
DK	Dänemark	LR	Liberia	SG	Singapur		
EE	Estland						

### **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  $2^{64}$  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  $x_0, x_1, \dots, x_n$  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  $x_{0,c}$  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 dargestellten 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 Komponente 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  $x_{0,c}$  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 benutzte 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 zugehörigen 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 zugehörige 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  $x_{0,c}$  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, kann ein Unbefugter auch bei Kenntnis von  $x_{0,C}$  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 Kryptoalgorithmen 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  $x_0, x_1, \dots, x_n$  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.

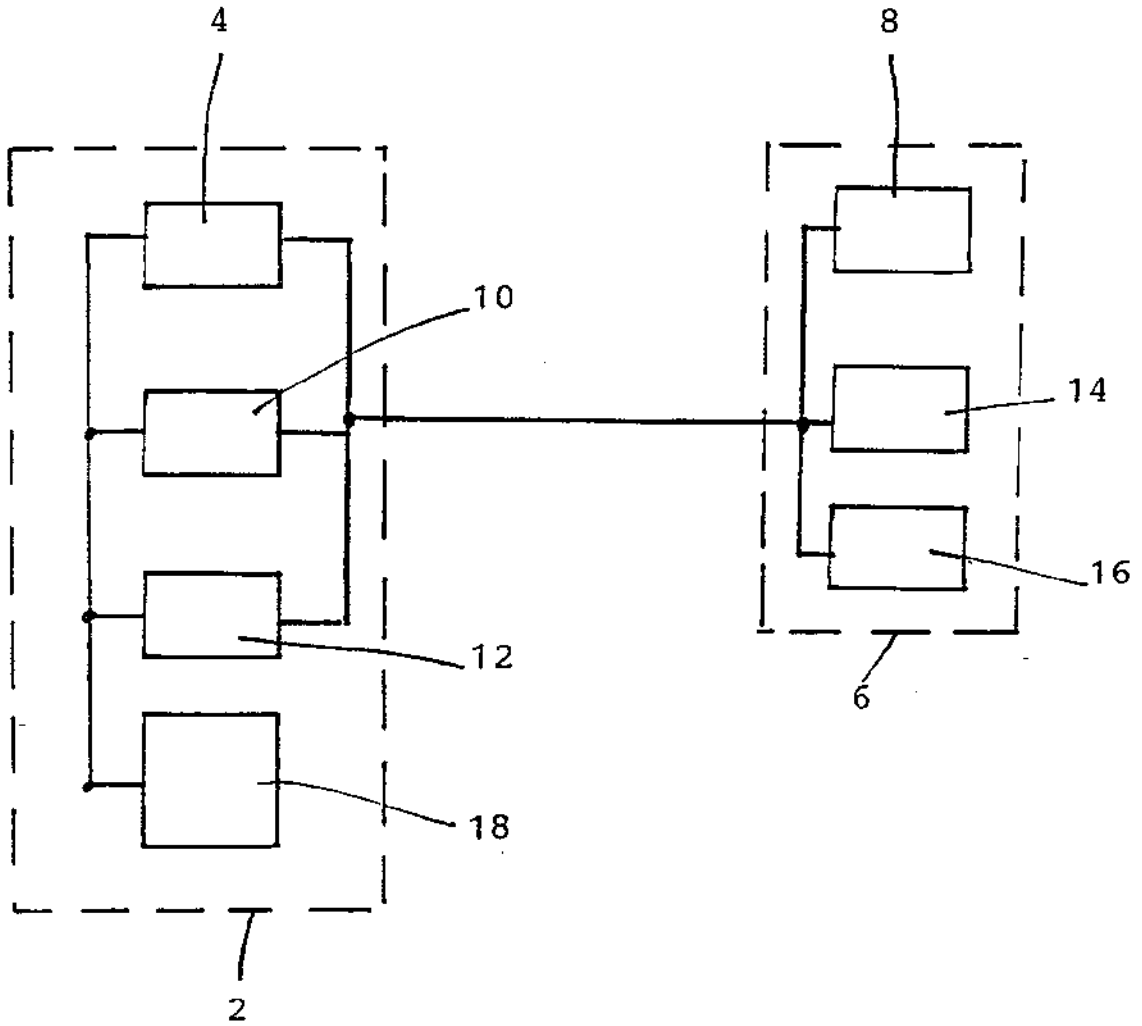
6. Verfahren nach einem der Ansprüche 1 bis 5, dadurch gekennzeichnet, daß die zugrundeliegende Verschlüsselungsfunktion oder Entschlüsselungsfunktion durch den geheimen Schlüsselwert parametrisiert ist.
7. Verfahren nach einem der Ansprüche 1 bis 6, dadurch gekennzeichnet, daß auf der Rechnerseite eine 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.



# INTERNATIONAL SEARCH REPORT

Inter. 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
- "F" 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 eps nl,  
 Fax: (+31-70) 340-3016

Authorized officer

Weiss, P

# INTERNATIONAL SEARCH REPORT

Information on patent family members

Inter. Appl. Application No

PCT/EP 99/00250

Patent document cited in search report	A	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**

Recherchiertes Mindestprüfstoff (Klassifikationssystem und Klassifikationsymbole)

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 z.B. geführt)

"O" Veröffentlichung, die sich auf eine mündliche Offenbarung, eine Ausstellung, 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 erfinderscher Tätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderscher 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 nahelegend ist

"Z" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

28. Juni 1999

Absenddatum 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

# 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 JP 8007720 B JP 63073348 A CA 1298653 A DE 3784824 A DE 3784824 T US 4853522 A	02-09-1996 29-01-1996 02-04-1988 07-04-1992 22-04-1993 11-09-1997 01-08-1989

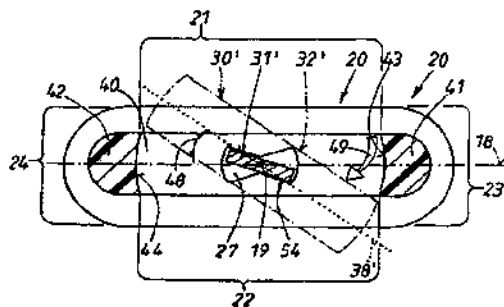




<b>(51) Internationale Patentklassifikation <sup>7</sup> :</b> <b>E05B 49/00, 19/00</b>	<b>A1</b>	<b>(11) Internationale Veröffentlichungsnummer: WO 00/36252</b>  <b>(43) Internationales Veröffentlichungsdatum:</b> 22. Juni 2000 (22.06.00)
<b>(21) Internationales Aktenzeichen:</b> PCT/EP99/09251 <b>(22) Internationales Anmeldedatum:</b> 29. November 1999 (29.11.99)  <b>(30) Prioritätsdaten:</b> 198 58 165.3      16. Dezember 1998 (16.12.98)    DE  <b>(71) Anmelder (für alle Bestimmungsstaaten ausser US):</b> HUF HÜLSBECK & FÜRST GMBH & CO. KG [DE/DE]; Steeger Strasse 17, D-42551 Velbert (DE).  <b>(72) Erfinder; und</b> <b>(75) Erfinder/Anmelder (nur für US):</b> JACOB, Dirk [DE/DE]; Breslauer Strasse 13, D-42579 Heiligenhaus (DE).  <b>(74) Anwalt:</b> MENTZEL, Norbert; Kleiner Werth 34, D-42275 Wuppertal (DE).	<b>(81) Bestimmungsstaaten:</b> AU, BR, CN, IN, JP, KR, US, eu- ropäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).  <b>Veröffentlicht</b> <i>Mit internationalem Recherchenbericht.</i>	

**(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 elektronischen 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 Schlüssel 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	ML	Mali	TR	Türkei
BG	Bulgarien	HU	Ungarn	MN	Mongolei	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MR	Mauretanien	UA	Ukraine
BR	Brasilien	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Island	MX	Mexiko	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	NE	Niger	UZ	Usbekistan
CF	Zentralafrikanische Republik	JP	Japan	NL	Niederlande	VN	Vietnam
CG	Kongo	KE	Kenia	NO	Norwegen	YU	Jugoslawien
CH	Schweiz	KG	Kirgisistan	NZ	Neuseeland	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	PL	Polen		
CM	Kamerun	KR	Republik Korea	PT	Portugal		
CN	China	KZ	Kasachstan	RO	Rumänien		
CU	Kuba	LC	St. Lucia	RU	Russische Föderation		
CZ	Tschechische Republik	LI	Liechtenstein	SD	Sudan		
DE	Deutschland	LK	Sri Lanka	SE	Schweden		
DK	Dänemark	LR	Liberia	SG	Singapur		
EE	Estland						

---

## 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 einem 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 Längsmittlinie 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 Längsmittle 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 Gehäuselängsmittellinie 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 Schlüsselenschaft 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 Herausziehpeils 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 zusammengefügteten 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)

## P a t e n t a n s p r ü c h e :

- 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,

d a d u r c h g e k e n n z e i c h n e t ,

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 Kopfbende (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 Ausbruchs (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 Längsmittle (16) des Gehäuses (20) angeordnet ist
- und dass die Längsmittle (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 Gabelschenkel (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 flexible 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.

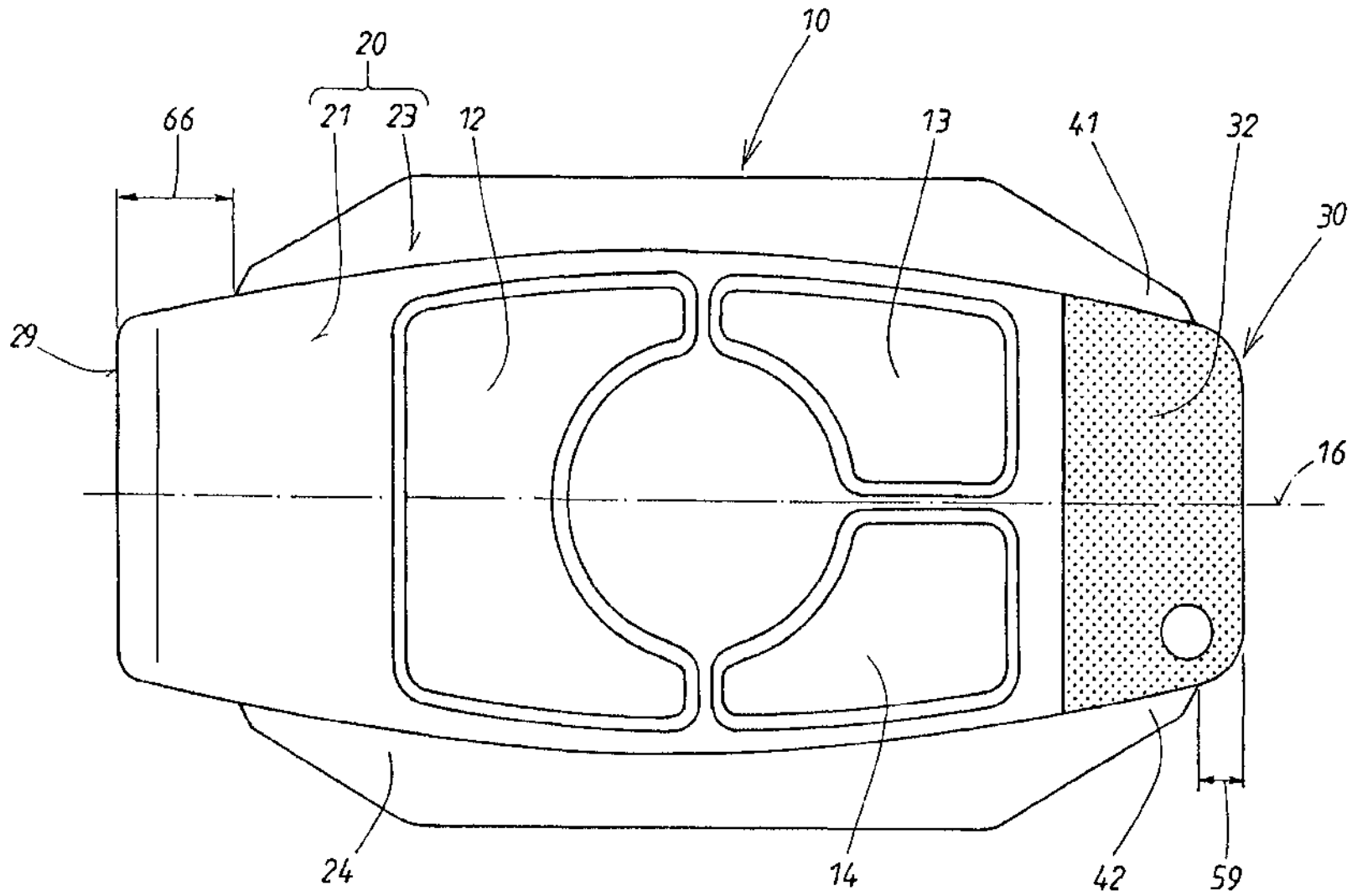


FIG. 1

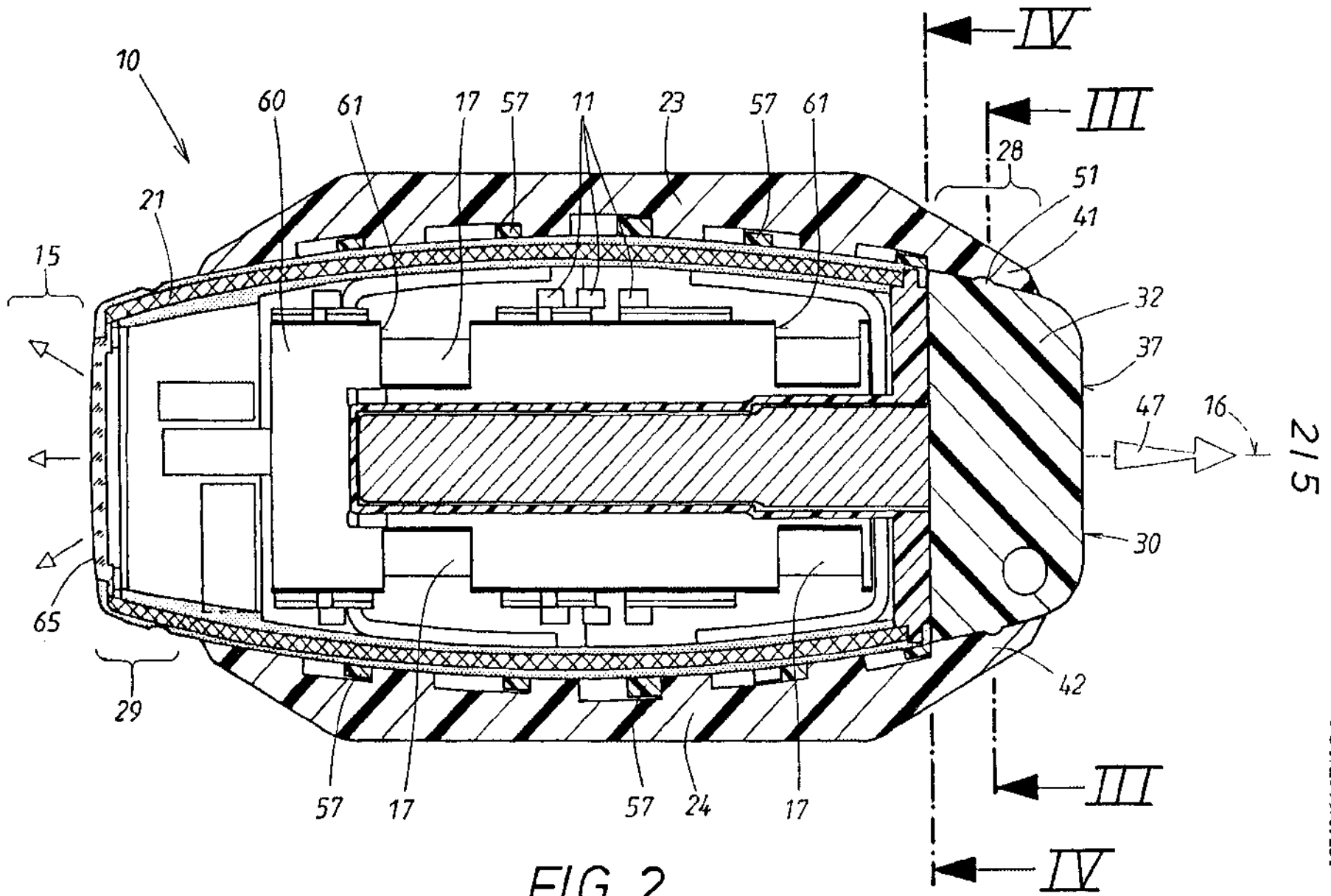


FIG. 2

315

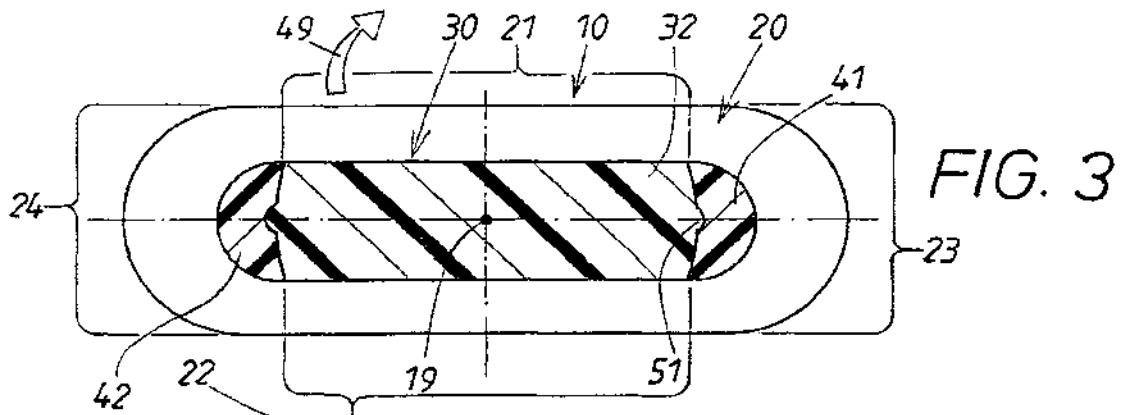


FIG. 3

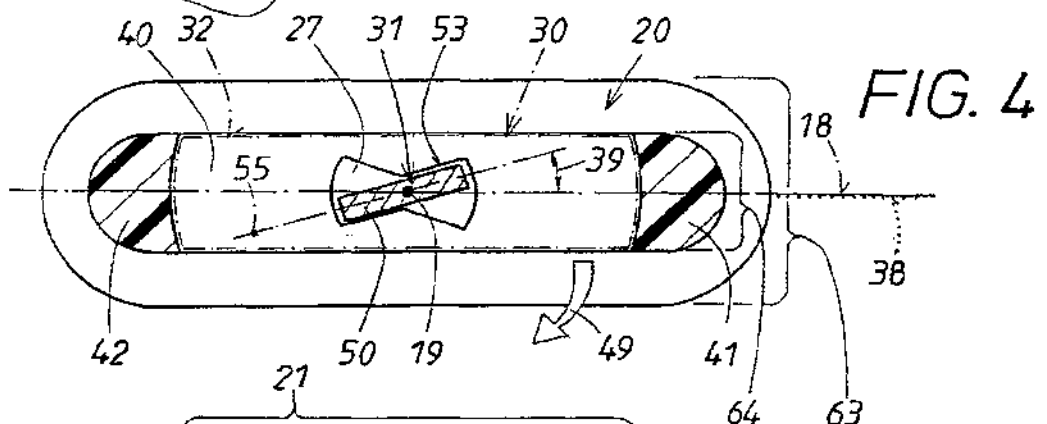


FIG. 4

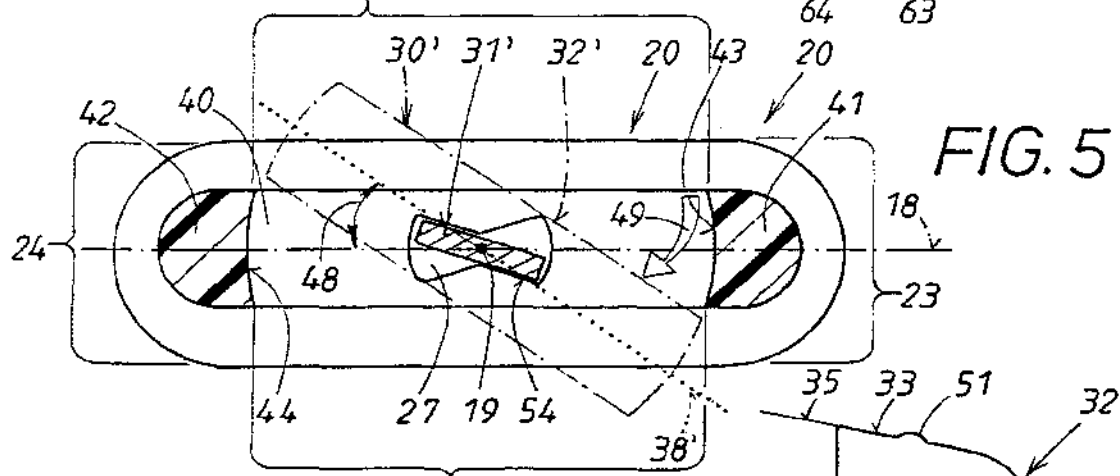


FIG. 5

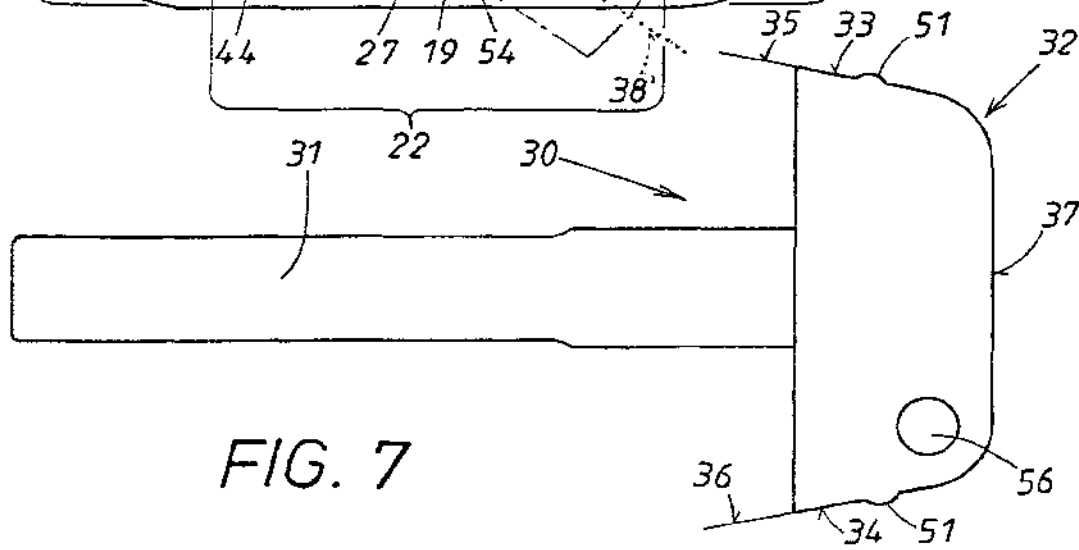


FIG. 7

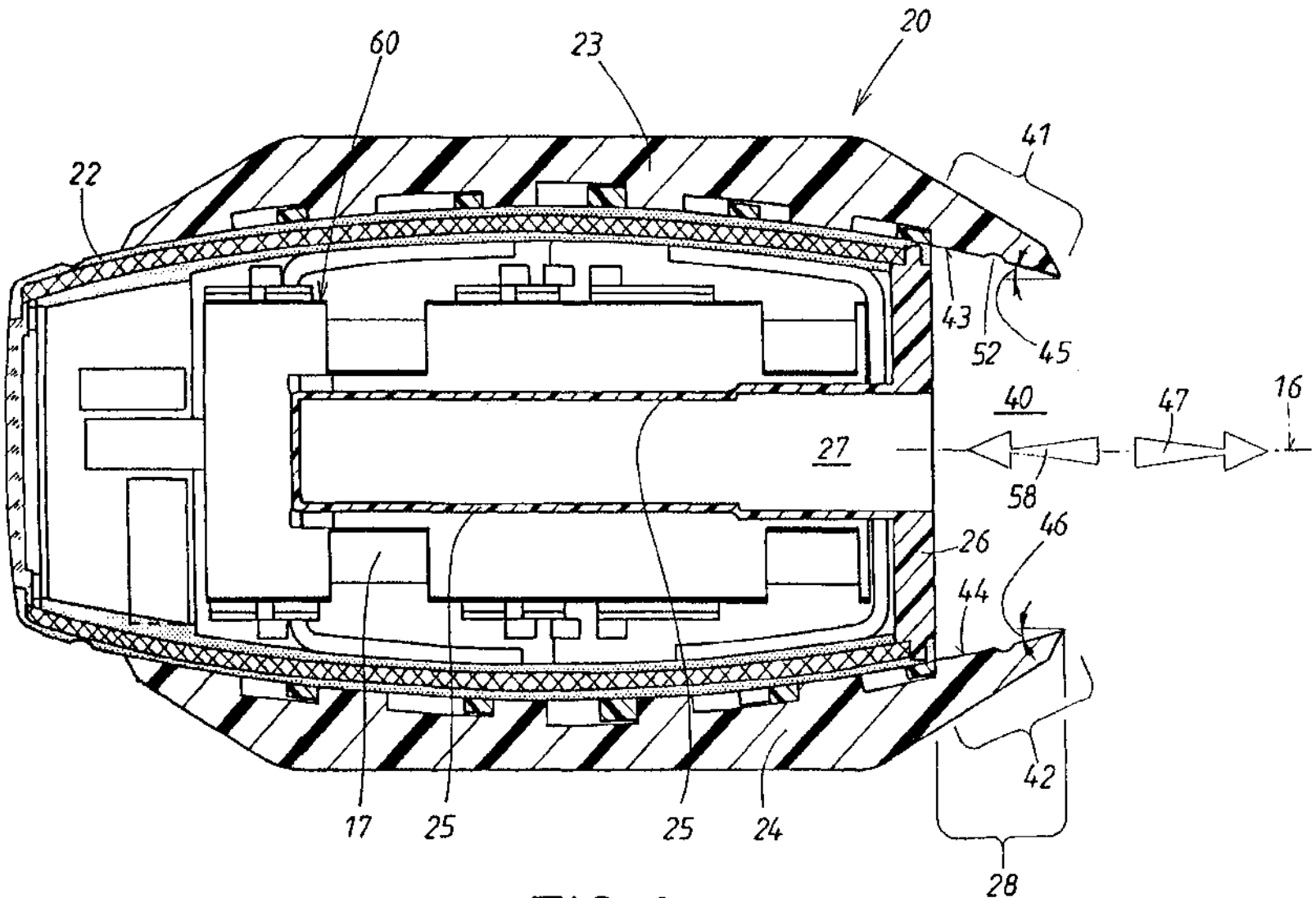


FIG. 6

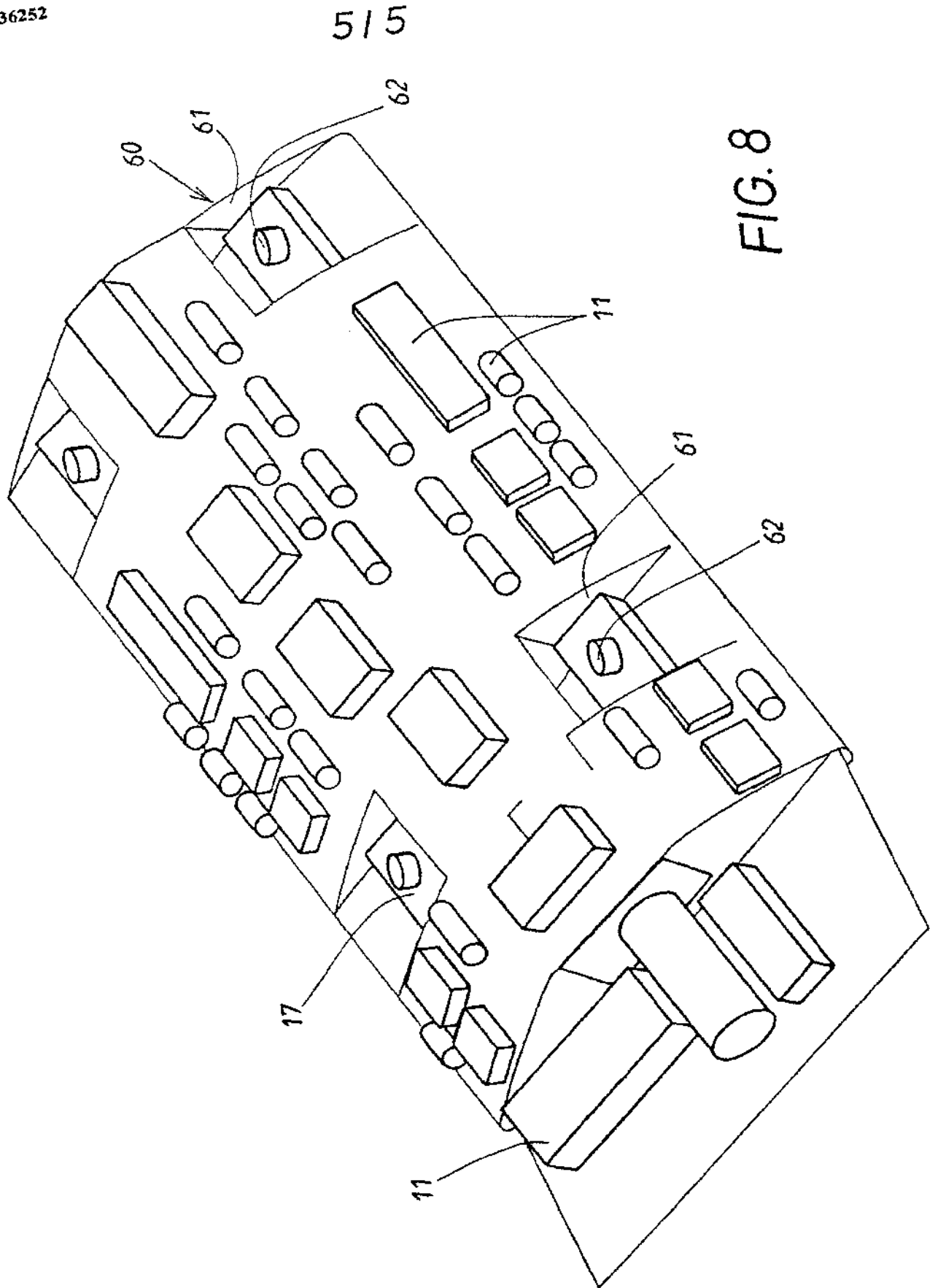


FIG. 8

INTERNATIONAL SEARCH REPORT

International 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,  
Fac (+31-70) 340-3018

Authorized officer

Buron, E



# INTERNATIONAL SEARCH REPORT

Information on patent family members

International 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

Inn. Internationales 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. RESEARCHIERTE GEBIETE**

Recherchiertes 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 erfindertätigkeit beruhend betrachtet werden

"Y" Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfindertätigkeit 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

"Z" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

16. Februar 2000

Abenddatum des internationalen Recherchenberichts

24/02/2000

Name und Postanschrift der internationalen Recherchenbehörde  
 Europäisches Patentamt, P.B. 5818 Patentaan 2  
 NL - 2200 HV Rijswijk  
 Tel. (+31-70) 340-2040, Tx. 31 051 epo nl,  
 Fax (+31-70) 340-3018

Bevollmächtigter Bediensteter

Buron, E

# INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP 99/09251

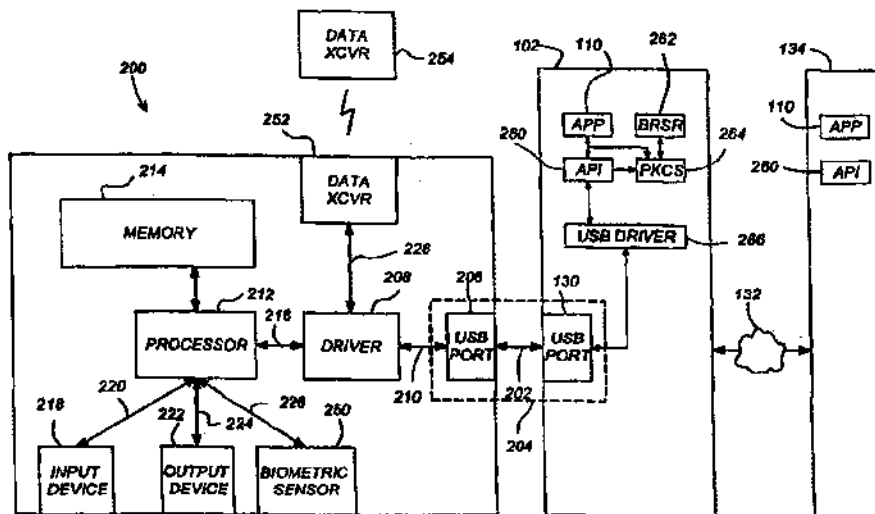
Im Recherchenbericht angeführtes Patentedokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 29722484 U	26-02-1998	KEINE	
DE 4444913 A	22-06-1995	KEINE	
DE 19723039 A	03-12-1998	KEINE	



INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

<p>(51) International Patent Classification <sup>7</sup> : <b>G06F 1/00</b></p>	<p><b>A1</b></p>	<p>(11) International Publication Number: <b>WO 00/42491</b> (43) International Publication Date: 20 July 2000 (20.07.00)</p>
<p>(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 &amp; Cooper, Suite 1050, 6701 Center Drive, West, Los Angeles, CA 90025 (US).</p>		<p>(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).</p> <p><b>Published</b> <i>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.</i></p>

(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.

<b>AL</b>	Albania	<b>ES</b>	Spain	<b>LS</b>	Lesotho	<b>SI</b>	Slovenia
<b>AM</b>	Armenia	<b>FI</b>	Finland	<b>LT</b>	Lithuania	<b>SK</b>	Slovakia
<b>AT</b>	Austria	<b>FR</b>	France	<b>LU</b>	Luxembourg	<b>SN</b>	Senegal
<b>AU</b>	Australia	<b>GA</b>	Gabon	<b>LV</b>	Latvia	<b>SZ</b>	Swaziland
<b>AZ</b>	Azerbaijan	<b>GB</b>	United Kingdom	<b>MC</b>	Monaco	<b>TD</b>	Chad
<b>BA</b>	Bosnia and Herzegovina	<b>GE</b>	Georgia	<b>MD</b>	Republic of Moldova	<b>TG</b>	Togo
<b>BB</b>	Barbados	<b>GH</b>	Ghana	<b>MG</b>	Madagascar	<b>TJ</b>	Tajikistan
<b>BE</b>	Belgium	<b>GN</b>	Guinea	<b>MK</b>	The former Yugoslav Republic of Macedonia	<b>TM</b>	Turkmenistan
<b>BF</b>	Burkina Faso	<b>GR</b>	Greece			<b>TR</b>	Turkey
<b>BG</b>	Bulgaria	<b>HU</b>	Hungary	<b>ML</b>	Mali	<b>TT</b>	Trinidad and Tobago
<b>BJ</b>	Benin	<b>IE</b>	Ireland	<b>MN</b>	Mongolia	<b>UA</b>	Ukraine
<b>BR</b>	Brazil	<b>IL</b>	Israel	<b>MR</b>	Mauritania	<b>UG</b>	Uganda
<b>BY</b>	Belarus	<b>IS</b>	Iceland	<b>MW</b>	Malawi	<b>US</b>	United States of America
<b>CA</b>	Canada	<b>IT</b>	Italy	<b>MX</b>	Mexico	<b>UZ</b>	Uzbekistan
<b>CF</b>	Central African Republic	<b>JP</b>	Japan	<b>NE</b>	Niger	<b>VN</b>	Viet Nam
<b>CG</b>	Congo	<b>KE</b>	Kenya	<b>NL</b>	Netherlands	<b>YU</b>	Yugoslavia
<b>CH</b>	Switzerland	<b>KG</b>	Kyrgyzstan	<b>NO</b>	Norway	<b>ZW</b>	Zimbabwe
<b>CI</b>	Côte d'Ivoire	<b>KP</b>	Democratic People's Republic of Korea	<b>NZ</b>	New Zealand		
<b>CM</b>	Cameroon	<b>KR</b>	Republic of Korea	<b>PL</b>	Poland		
<b>CN</b>	China	<b>KZ</b>	Kazakstan	<b>PT</b>	Portugal		
<b>CU</b>	Cuba	<b>LC</b>	Saint Lucia	<b>RO</b>	Romania		
<b>CZ</b>	Czech Republic	<b>LI</b>	Liechtenstein	<b>RU</b>	Russian Federation		
<b>DE</b>	Germany	<b>LK</b>	Sri Lanka	<b>SD</b>	Sudan		
<b>DK</b>	Denmark	<b>LR</b>	Liberia	<b>SF</b>	Sweden		
<b>EE</b>	Estonia			<b>SG</b>	Singapore		

USB-COMPLIANT PERSONAL KEY WITH  
INTEGRAL INPUT AND OUTPUT DEVICES

5

10

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.

15

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.

20

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

25

(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  
5 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  
10 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.

15 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  
20 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  
25 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  
5 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.  
10 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  
15 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  
20 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  
25 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  
30 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  
5 maider 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  
10 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  
15 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  
20 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,  
25 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-  
30 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 transection 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);
- 5     • 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);
- 10    • 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)
- 15    • 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-  
20 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  
25 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.

30

### 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  
5 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  
10 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  
15 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  
20 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  
25 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  
30 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  
5 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  
10 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  
15 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  
20 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  
25 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  
30 264 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  
5 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  
10 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  
15 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  
20 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  
25 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  
30 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  
5 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  
10 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  
15 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  
20 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  
25 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  
30 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  
5 316 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  
10 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  
15 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  
20 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.

25 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  
30 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  
5 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  
10 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  
15 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.  
20 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  
25 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  
30 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

5 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

10

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

5

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.

10

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  
 5 implement a secure document access system. This secure document access system provides remote users access to secret encrypted documents over the Internet to company employees. 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  
 10 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

be created. The global create and delete access types are then set to the master key using the SetAccessSettings command. The DOCFilename database is then loaded in the personal key 200, and the CreateDir and CreateFile APIs 260 are used as required to create and allocate directories and files. The SelectFile, WriteFile, and CloseFile  
5 API commands are used to load the files and the secret. Depending on whether access is to be limited to a particular number of occasions, the DATA or CTR file types are used.

The BUILDDOC program is used to accept new documents into the secure access library. Using information from the personal key 200, encryption keys are  
10 generated that are used by a document encryption engine in the personal key 200.

The BUILDDOC program is a stand-alone application that runs on trusted systems within the secure walls of the organization. It requires validation of the master key. It uses the personal key 200 to create an encryption key for each document file name.

15 First, the HashToken API 260 with the XOR option is used to hash together the DOCFilename, block number (computed by the BUILDDOC program as it reads and encrypts the document), DOCSecret. The block number is calculated by the BUILDDOC program as it reads and encrypts the document. The resulting MD5-XOR digest is used as the encryption key that is used by the encryption engine in the  
20 BUILDDOC application. Then, the CreateFile, SelectFile, WriteFile, and CloseFile APIs 260 along with the HashToken in XOR mode are used on each document that is to be added to the secure document library.

The VIEWDOC program is a web browser 262 plug-in application allows the user to open, decrypt, and view the document based on his/her personal key 200 based  
25 document access codes. If desired, the view counters for some types of documents can also be decremented in the VIEWDOC program. The VIEWDOC program does not require file saving or forwarding, screen scraping, and printing.

The VIEWDOC program validates the user and uploads and decrypts the documents. It uses the VerifyPIN command API 260 to authenticate the user. The

user can then view the documents listed in the personal key 200 directory as long as the personal key 200 remains communicatively coupled to the USB port 130.

A message facility, such as the message facility used in the WINDOWS operating system (WM\_DEVICECHANGE) can be used to determine if the key has  
5 been removed. The Dir, SelectFile, ReadFile, and CloseFile command APIs 260 are used to determine which documents can be read. The HashToken with the XOR mode API 260 along with DOCSecret, DOCFilename, and the document block numbers are used to create the decryption key on a per block basis. When the DOCfilename is of file type CTR, the CTR is decremented using the Decrement  
10 command API 260. In one embodiment, to reduce complexity, the CTR field is not hashed, but merely managed by VIEWDOC.

The LIBDOC program provides an administrative function that is a subset of SETKEY. It allows a secure document librarian to grant access to documents based upon information stored in the personal key 200. The net effect is that the trusted  
15 librarian can update the personal key 200 based list of documents that can be viewed.

The LIBDOC program updates the list of DOCFilenames on a per-personal key 200 basis. After verifying the master key with VerifyMasterKey command API 260 and looking the user name up in the employee data base, the current set of DOCFilenames are updated using the SelectFile, WriteFile, and CloseFile command  
20 APIs 260.

Using the foregoing, employees worldwide can carry a personal key 200 loaded with their local database of file names. Individual departments do not have to rely on MIS procedures to restrict who has access to documents. The personal keys 200 of department members can be updated using the LIBDOC program as required.  
25 Documents can be decrypted and viewed by the employees only if the personal key 200 secret is correct. The personal secret remains secure because it is never revealed outside of the personal key 200. A simple form of metering can also be used to reduce the number of copies of documents that can be used to reduce the number of copies of documents that can be viewed.



FIG. 6 is a diagram presenting an illustration of one embodiment of the personal key 200. The personal key 200 comprises a first housing member 602 and a second housing member 604. The first housing member 602 is sized and shaped so as to accept a circuit board 606 therein.

5           The first housing member 602 comprises a plurality of bosses 624, which, when inserted into each respective hole 640 in the second housing member 604, secures the first housing member 602 to the second housing member 604. The first housing member 602 and the second housing member 604 also each comprise an aperture 628, which allows the personal key 200 to be affixed to a key chain.

10           The circuit board 606 is held in position by a plurality of circuit board supports 608. The circuit board 606 comprises a substantially flat circuit connection surface 610 on the periphery of the circuit board 606 for communicative coupling with the host processing device or computer 102 via conductive pins. Circuit connection surface 610 allows communication with a processor 212 mounted on the circuit board  
15 606. The processor 212 comprises memory and instructions for performing the operations required to implement the functionality of the personal key 200 as disclosed herein. The processor is communicatively coupled with a memory 214 on the circuit board to store and retrieve data as required by processor 212 instructions. In the illustrated embodiment, the circuit board 606 also comprises an output device  
20 222 such as a light emitting device 616, e.g. light emitting diode (LED), which provides the user of the personal key 200 a visual indication of the operations being performed by the personal key 200. This is accomplished, for example, by emitting light according to a signal passing from the host computer 102 to the personal key 200. The light emitting device could also comprise a liquid crystal display (LCD) or  
25 other device providing a visual indication of the functions being performed in the personal key or data passing to or from the personal key 200.

          The energy from the light emitting device 616 is presented to the user in one of two ways. In the embodiment illustrated in FIG. 2, the light emitting device 616 is disposed through a light emitting device orifice 644 in the second housing member  
30 604. In this design, the personal key 200 can be sealed with the addition of a small

amount of epoxy or other suitable material placed in the light emitting device orifice 644 after assembly.

In another embodiment, the light emitting device 616 does not extend beyond the interior of the housing 602, 604, and remains internal to the personal key 200. In this embodiment, at least a portion of the first housing 602 or the second housing 604 is at least partially translucent to the energy being emitted by the light emitting device 616 at the bandwidths of interest. For example, if the light emitting device 616 were a simple LED, the second housing 604 can be selected of a material that is translucent at visual wavelengths. One advantage of the foregoing embodiment is that the LED can be placed where it does not allow electromagnetic discharges and other undesirable energy to the circuit board 606 or any of the components disposed thereon. This is because no part of the LED, even the surface, is in contact with the user's hand at any time.

While the foregoing has been described with a single light emitting device 646, the present invention can also advantageously embody two or more light emitting devices, or devices emitting energy in other wavelengths. For example, the foregoing can be implemented with a three color LED (red, yellow and green), or three one-color LEDs to transfer personal key 200 information to the user.

In addition to or as an alternative to the foregoing, information regarding the operation of the personal key 200 is provided by an aural transducer such as a miniaturized loudspeaker or piezoelectric transducer. Such aural information would be particularly beneficial to users with limited or no vision. For example, the aural transducer can be used to indicate that the personal key 200 has been inserted properly into the host computer 120 I/O port 130.

An aural transducer may also be used to provide alert information to the user. This is particularly useful in situations where the user is not expecting any input or information from the key. For example, if the personal key 200 or related device is engaged in lengthy computations, the aural transducer can indicate when the process is complete. Also, the aural transducer can indicate when there has been an internal fault, when there has been an attempt to compromise the security of the key with

infected or otherwise harmful software instructions, or to prompt the user to take an action such as providing an input to the key 200.

Further, it is envisioned that as the use of personal keys 200 will become widespread, it will be beneficial to incorporate the functions of other devices within  
5 the personal key. For example, a device such as a paging transceiver can be incorporated into the personal key to allow the user to be summoned or contacted remotely. Or, the personal key 200 may be used to store programs and instructions such as the user's calendar. In this application, the personal key 200 can be used to remind the user of events on the calendar, especially in conjunction with the LCD  
10 display discussed above. The aural transducer can be operated at a wide variety of frequencies, including minimally audible vibrational frequencies. This design is particularly beneficial, since the personal key is small enough to be placed on the user's key ring, where it will be in pocket or purse for lengthy periods of time where it cannot be seen or easily heard.

15 FIGs. 7A-7C are diagrams showing one embodiment of the personal key 200 having an input device 218 including a first pressure sensitive device 702 and a second pressure sensitive device 704, each communicatively coupled the processor 212 by a communication path distinct from the USB-compliant interface 204.

FIG. 7A illustrates an embodiment of the personal key 200 in which an output  
20 device 222 such as an LED or LCD display 706 is communicatively coupled to the processor 212 by a second communication path distinct from the USB-compliant interface 204. In this embodiment, input to the personal key processor 212 may be supplied by depressing a combination of the pressure sensitive devices 702, 704, optionally as directed by the output device 222.

25 In an embodiment illustrated in FIGs. 7B and 7C, the pressure sensitive devices 702 and 704 are simple mechanical push switches communicatively coupled to the processor 212 via traces on the circuit board 606. In this case, the switches 702 and 704 may be actuated by depressing a button surface that extends through apertures 708 and 710 in the second housing member 604. FIG. 7B also shows a window 712  
30 permitting viewing of the output device 706 display.

FIG. 7C shows the exterior appearance of this embodiment of the personal key 200 when the first housing member 602 and the second housing member 604 are assembled.

In another embodiment of the present invention, the pressure switches 702 and 704 do not extend to the exterior of the personal key 200. Instead, the personal key 200 is configured so that pressure may be exerted on the pressure sensitive switches 702 and 704 without requiring any portion of the switches to extend to the exterior of the personal key 200. For example, in one embodiment, at least a portion of the exterior surface of the personal key 200 is sufficiently flexible to permit pressure exerted on the outside surface of the key 200 to actuate the switches therein. Alternatively, the first housing member 602 and the second housing member 604 may be hinged to allow pressure to be applied to the switch. In another embodiment, the thresholded output of a pressure sensitive device such as a strain gauge is used to indicate user input to the personal key.

The foregoing pressure sensitive devices 702 and 704 may be used as follows. In one embodiment, the two pressure sensitive devices 702 and 704 is used to enter alphanumeric information. Here, pressure can be applied to the first pressure sensitive device 702 to select the desired character. To assist the user, the currently selected character can be displayed on the output device 222. When the user is satisfied with the selected character, applying pressure to the second pressure sensitive device may indicate that the currently displayed character should be entered (thus providing an "enter" function). This process may be repeated until all of the characters of the user input (e.g. a user password or personal identification number (PIN)) has been entered. The end of the user input can be signified by repeated application of pressure to the second pressure sensitive device 702, and confirmed by the output device 222. An aural transducer can be used alone or in combination with a visual display to indicate the character, to indicate an error, or to indicate when the user input process has been completed.

The foregoing pressure sensitive devices may also be used to provide a binary input to the personal key 200. For example, the user's PIN or password can be

entered by applying pressure to the first pressure sensitive device 702 and the second pressure sensitive device 704 in the proper order in rapid succession. In this way, a user password or PIN defined as "10100010111" may be entered by depressing the first pressure sensitive device 502 to indicate a "0" and the second pressure sensitive device 704 to indicate a "1."

FIGs. 8A-8C are diagrams presenting an illustration of another embodiment of the present invention. In this embodiment, the input device 218 comprises an edge exposed wheel 802 coupled to the processor by the input device communication path 808. In this embodiment, the user provides an input by urging the wheel 802 through a series of tactile positions identifying input characters. When the desired input character is either shown on the output device 222 or on the wheel 802 itself, the user can indicate the character as a user input by urging the wheel 802 toward the centerline of the personal key 200. This process can be repeated for a series of input characters, until all of the desired characters are provided. The user can also indicate that no more input will be provided by urging the wheel 802 toward the center of the personal key multiple times in rapid succession, or by selecting an input tactile position on the wheel 802 and depressing the wheel 802.

#### Security Features Using the Input and Output Devices

The input device 218 and output device 222 of the present invention can be advantageously used to enhance the security of the personal key 200. For example, when connected to the host computer 102, the personal key 200 can be used to authorize transactions with a remote computer/server 134 communicatively coupled to the host computer 102 via a communication medium 132 such as a dial-up network, the Internet, LAN, or WAN. Malicious software, which can be executing in the remote computer/server 134 or the host computer 102, can send anything it wants to the personal key 200 for authorization without the knowledge or permission of the user. Without some sort of user input device 218, the personal key 200 can authorize transactions without the user's knowledge that the holder cannot repudiate. Such transactions may include, for example, payment and legally binding signatures.

Although a personal identification such as the personal identification number (PIN) is required to log on and activate the personal key 200, the personal key 200 ordinarily remains active once the PIN has been entered. Hence, the personal key 200 will perform any action for any application, without notice to, or authorization by the user.

To ameliorate this problem, one embodiment of the present invention utilizes a "squeeze to sign" authorization technique, in which some direct user action is required to authorize the use of identified secret values stored in the personal key 200. For instance, if a private key (such as the secret 406) or PIN stored in the memory 214 of the personal key 200 is identified as requiring a "squeeze to sign" authorization, firmware executing in the processor 212 of the personal key 200 requires direct user input via the input device 410 or the data transceiver 252 before honoring any request from the host computer 102 or the remote computer/server 134 that involves the use of the private key or personal information. Ordinarily, the private key and/or other personal information is designated as requiring direct authorization by an associated value or flag in the memory 214. Such data may also be designated as "use-only" indicating that the data cannot be read directly from the key under any circumstances. The data may be shared with no other entity (as would often be the case with a PIN), or may be a value shared with the trusted entity and used for authorization, such as the secret 406. For example, private keys can be used as the secret 406 to perform authorization via hash functions. In such cases, the secret value 406 is typically a shared secret such as a DES key or a password. Since secret values 406 can be stored in the memory 214 of the personal key 200, before distributing the personal key 200 to the user, the secret value 406 need not be made available in plaintext form at any time.

Typically, each time a user connects to an SSL secured web site that supports client authentication, a browser 262 calls middleware such as one of the APIs 260 or the PKCS 264, which commands the personal key 200 to encrypt a challenge value with the user's secret private key 406B (stored in the personal key memory 214). Assuming the user's PIN is already stored in the personal key 200, thus authenticating the user to the personal key 200, it still remains to authenticate the key to the secure

web site. In this case, access to the user's secret private key is required, and the output device 222 integrated with the personal key 200 may activate to indicate that a command that requires access to the private key has been invoked, and that the user needs to authorize this access. In one embodiment of the present invention this is accomplished by blinking a visual output device (such as an LED or LCD display), or by beeping an aural device. In another embodiment of the present invention, the middleware (either the API 260 or the PKCS 264) activates the display 122 attached to the computer 102, indicating that the user must authorize access to the private key before processing can proceed. An input device 218 in the personal key 200 such as the wheel 802 or one of the pressure sensitive devices 702 and 704 can then be actuated by the user to indicate that the user has authorized access to the private key. No authorization is granted if the personal key 200 is removed from the I/O port 130, or a "cancel" button presented on the display 122 is selected to refuse the on-screen dialogue. Access to the private key (in the example above, to perform the hash function) is granted if the user authorizes as such. The "squeeze to sign" concept thus makes it less likely that malicious software will be able to use the secret 406B without the user's consent or knowledge.

Malicious software may monitor the interface between the personal key 200 and the host computer 102 to capture the value of user's PIN. Although the PIN cannot be read directly, it is possible for the malicious software to examine both the VerifyPIN command described in Table 6 (and its argument) and the response from the personal key 200. If the response indicates that the proper PIN was provided as an argument to the VerifyPIN command, the malicious software can determine the PIN itself. The foregoing can also be applied to further safeguard the user's PIN instead of the secret 406B. For example, if a sniffer module in malicious software in the host computer has been able to access the user's PIN, when it attempted to use that PIN in a context the user did not expect, the user would be alerted to the fact that the PIN had been compromised.

FIG. 9 is a flow chart illustrating an embodiment of the present invention in which processor 212 operations are subject to user authorization. First, the API 260

issues 902 a command that invokes a processor 212 operation. The command is transmitted via the USB-interface 204 to the personal key 200. The processor 212 accepts the command, as shown in block 904. The personal key 200 then determines whether the invoked processor command is one that requires authorization. This can  
5 be accomplished by storing information in the memory 214 of the personal key indicating which processor commands require authorization. For example, this can be implemented in a map stored in the memory 214, a plurality of flags, where it may be customized for each user, or the information can be stored in the processor 212  
10 firmware or similar location so that the mapping cannot be altered. In one embodiment, different levels of authorization are implemented for different processor commands (e.g. a write command may require authorization, whereas a read command may not).

In another embodiment, authorization may be premised on data instead of the invoked command, or on a combination of the invoked command and data. For  
15 example, the present invention may be configured to require authorization any time the PIN is accessed in any way, or when the PIN is read from the memory 214 of the personal key 200, but not when other data is read, or when the PIN is written to the personal key 200. This may be accomplished, for example, by determining which data stored in the memory 214 is affected by the processor operation, and determining  
20 whether the data affected by the processor operation is associated with an identification designating the data as private information.

Using one of the output devices 222, the data transceiver 252, or the display 122 coupled to the host computer, the personal key 200 may then prompt the user to authorize the processor operation, as shown in block 906. This may be accomplished  
25 by flashing a display device such as an LED or LCD, by activating an aural transducer, or by performing both operations. If desired, the user may be prompted first with a display device, and if the authorization is not forthcoming within a specified period of time, the aural transducer may be activated.

To expose the prompting operation as little as possible to malicious software  
30 or other intrusive activity, the prompt is preferably performed using a communication



path entirely distinct from the communication path between the personal key 200 and the host computer 102 (in the illustrated example) the USB-interface 204. To further increase security, the illustrated embodiment prompts the user with the output device 222 via a communication path which not manifested externally from the personal key  
5 in any way that is visible to the malicious software, and is hence not subject to tampering.

Next, the user provides an input signaling authorization of the operation 910. This can be performed using a variety of input devices, such as the mouse 116, or keyboard 114, but is preferably performed using an input device 218 or the data  
10 transceiver 252 in the personal key 200. This information is communicated to the personal key 200 via a communication path that is entirely distinct from the communication path between the personal key 200 and the host computer 102, and preferably entirely internal to the personal key 200 (not manifested externally to the personal key 200 by a means visible to malicious software). This prevents malicious  
15 software interfering with or emulating the user authorization.

Another embodiment of the present invention provides additional PIN security. In this embodiment, the VerifyPIN command is altered from that which is described in Table 6. Ordinarily, the VerifyPIN command accepts what the host computer 102 or remote computer/server 134 believes is the user's PIN as an  
20 argument. The personal key 200 accepts this command and returns a status indicating whether the proper PIN was provided. In this alternative embodiment however, the VerifyPIN command is altered so that it does not include the PIN as an argument. The VerifyPIN command is provided to the personal key 200, and the user is prompted to enter his or her PIN. After the PIN is entered, it is communicated to the processor 212  
25 via a communication path 220 which is distinct from the host computer 102 - personal key 200 interface, and not externally manifested anywhere where it can be detected by malicious software. It is then internally verified, and a message providing the result of that manifestation is transmitted from the personal key 200 to the host computer 200 or remote computer/server 134. This prevents any external manifestation of the PIN.

When combined with the hashing technique using the secret 406 above, the foregoing provides a highly secure technique for user authorization. The secure hashing technique authenticates the key, and protects the secret 406 from external exposure. However, the hashing technique does not authenticate the person  
5 possessing the key (since it may have been lost or stolen). The ability to enter the PIN directly into the processor 212 of the personal key allows the personal key to authenticate the user, and since the PIN is never manifested externally from the key, exposure to malicious software is prevented. Since the third party can authenticate the personal key and the personal key can authenticate the user, the third party can  
10 perform user authentication with a high degree of confidence.

FIG. 10 is a flow chart illustrating an embodiment of the present invention in which the PIN is entered directly into the personal key 200. In block 1002, a command is issued which requires access to the user's PIN, such as the VerifyPIN and ModifyPIN commands listed in Table 6. The personal key 200 accepts 1004 the  
15 command, and if necessary, prompts the user for the PIN, as shown in block 1006. This may be accomplished with the display 122, one of the output devices 222, or any combination thereof. Preferably, this is accomplished via a communication path distinct and inaccessible from the USB interface 204. Using one of the input device 218 embodiments described above, the user provides the PIN to the personal key 200.  
20 Using a value stored in the memory 214, the processor 212 in the personal key 200 validates the user-entered PIN. In one embodiment, this is accomplished by comparing the user-provided value directly with a value stored in the memory 214. The personal key then provides 1014 a response indicating the validity of the PIN, which is accepted by the API 260. The response indicates whether the user supplied  
25 PIN was valid.

In one embodiment, a biometric sensor 250 is also communicatively coupled to the processor 212. The biometric sensor 250 provides data to the processor 212 and receives commands from the processor 212, as described earlier in this disclosure.

The processor is also optionally communicatively coupled to one or more light  
30 emitting devices 216 or other visual display device to provide a visual indication of

the activities or status of the personal key 200. The processor 212 may also be communicatively coupled with an aural device to provide a vibrational or audio data to the user of the status or activities of the personal key 200.

5

### Conclusion

This concludes the description of the preferred embodiments of the present invention. In summary, the present invention describes a compact, self-contained, personal token. The token comprises a USB-compliant interface releasably 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.

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. For example, while the foregoing personal key has been described as providing for electrical communication with the host communication, it is envisioned that such electrical communication includes the optical transfer of data such as is implemented by fiber optics and the like.

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 (200), comprising:
  - a USB-compliant interface (206) releasably coupleable to a host processing device (102);
  - 5 a memory (214);
  - a processor (212), communicatively coupled to the memory (214) and communicatively coupleable to the host processing device (102) via the USB-compliant interface (130), the processor (212) for providing the host processing device (102) conditional access to data storable in the memory (214); and
  - 10 a user input device (218), communicatively coupled to the processor (212) by a path (220) distinct from the USB-compliant interface (206).
2. The apparatus of claim 1, wherein the user input device (218) is configured to control an operation of the processor (212).
- 15 3. The apparatus of claim 1, wherein the operation comprises an operation selected from the group comprising:
  - an encryption operation; and
  - a decryption operation.
- 20 4. The apparatus of claim 1, wherein the operation comprises a digital signature operation using a private key stored in the memory (214).
5. The apparatus of claim 1, wherein the input device (218) comprises at least one pressure-sensitive device actuatable from an exterior surface of the token (200).
- 25 6. The apparatus of claim 1, wherein the input device (218) comprises at least one push-button switch (702).

7. The apparatus of claim 1, further comprising an output device (222),  
communicatively coupled to the processor (212) by path (224) distinct from the USB-  
compliant interface (206), for providing information regarding the operation of the  
5 processor (212).

8. The apparatus of claim 7, wherein the output device (212) comprises at  
least one light emitting device (616).

10 9. The apparatus of claim 7, wherein the output device comprises at least  
one liquid crystal display (706).

10. The apparatus of claim 7, wherein the output device comprises at least  
one aural output device.

15

11. A compact personal token (200), comprising:  
a USB-compliant interface (206) releaseably coupleable to a host processing  
device (102);

a memory (214);

20

a processor (212), communicatively coupled to the memory (214) and  
communicatively coupleable to the host processing device (102) via the USB-  
compliant interface (206), the processor (212) for providing the host processing  
device (102) conditional access to data storable in the memory (214); and

a user output device (222), communicatively coupled to the processor (212).

25

12. The apparatus of claim 11, wherein the user output device (212) is  
coupled to the processor (212) by a path (224) distinct from the USB-compliant  
interface (206).

13. The apparatus of claim 11, wherein the user output device (212) is configured to indicate the operation of the processor (212).

14. The apparatus of claim 11, wherein the operation comprises an operation selected from the group comprising:  
5 an encryption operation;  
a decryption operation; and  
a digital signature operation using a private key.

15. The apparatus of claim 11, wherein the user output device (212) is selected from a group comprising:  
at least one light emitting device (616);  
at least one liquid crystal display (706); and  
at least one aural device.

16. The apparatus of claim 11, further comprising an input device (218), communicatively coupled to the processor (212) by path (220) distinct from the USB-compliant interface (206), for providing information for the operation of the processor (212).

17. The apparatus of claim 11, wherein the processor (212) and memory (214) are disposed on a circuit board (606) having at least one circuit connection surface (610) providing electrical communication with the processor (212), and the USB-compliant interface (206) comprises:

25 at least one conductive pin for providing electrical communication between the circuit connecting surface (610) and the host processing device (102), wherein the conductive pin comprises a pin securing portion and is releasably coupleable to the circuit connection surface (610); and

30 a housing (602) for substantially enclosing at least some of the circuit board(606), the housing (602) comprising a pin interfacing portion mateable with the pin securing portion for securing the pin member along a longitudinal axis of the conductive pin.

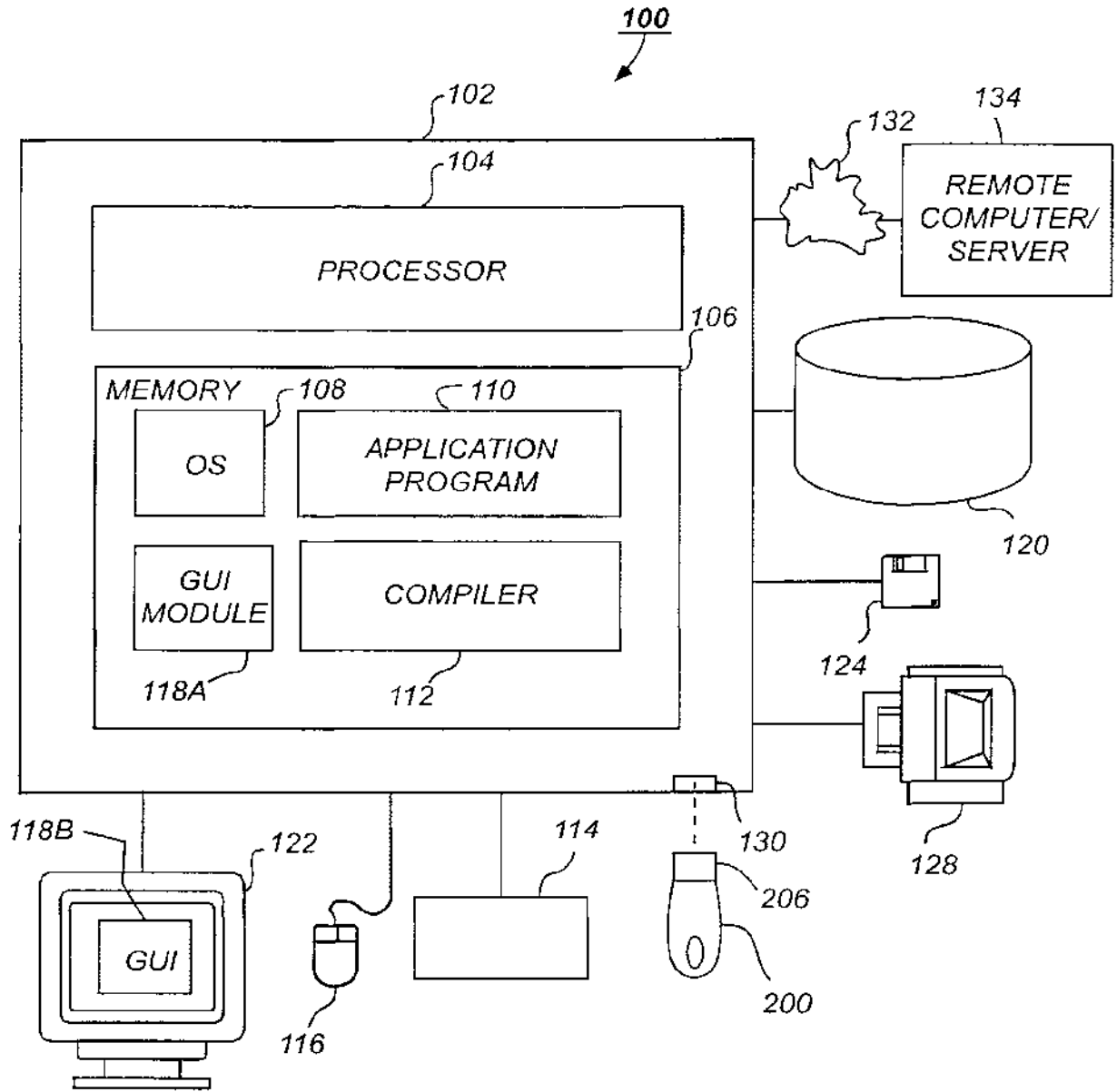


FIG. 1



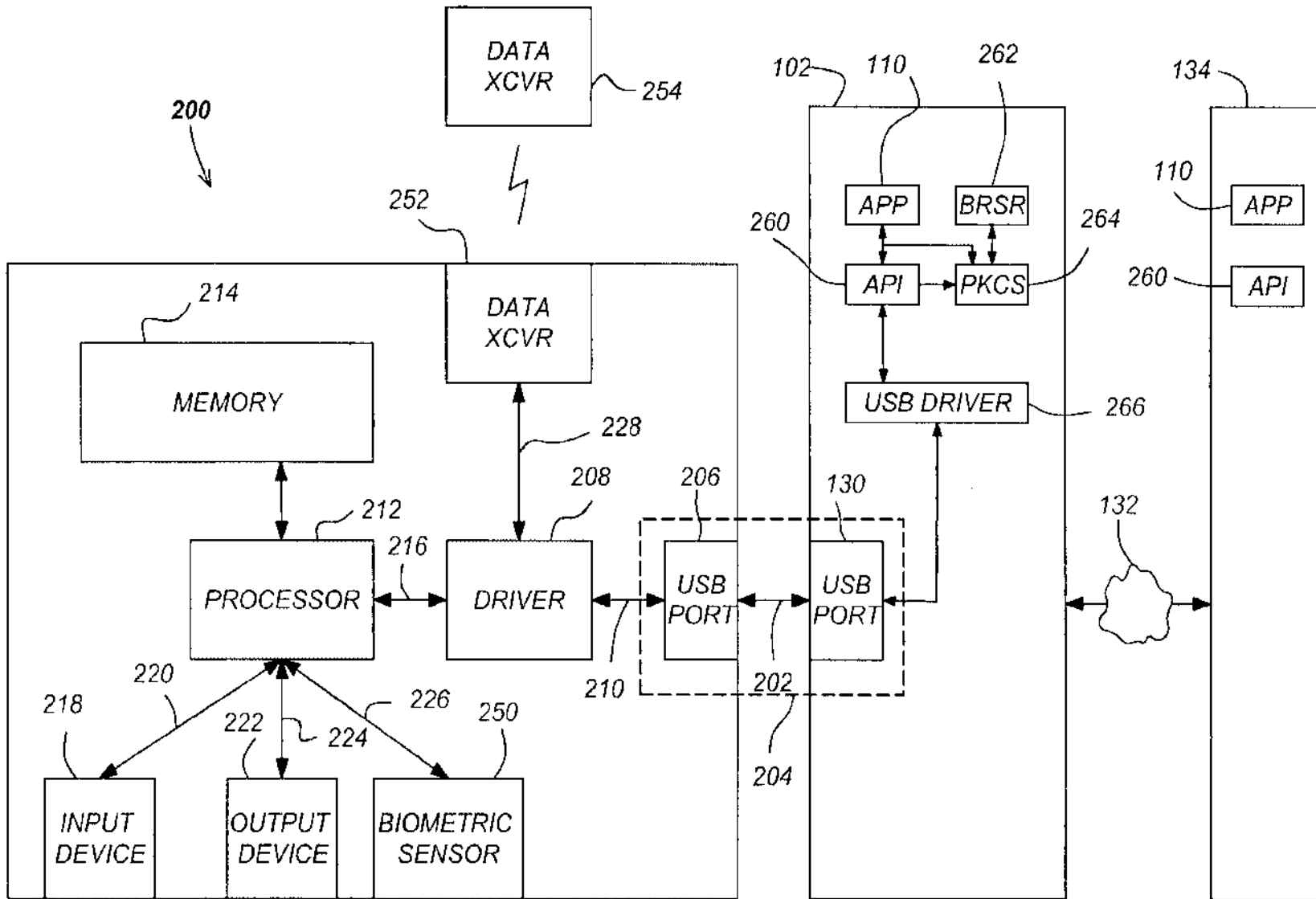


FIG. 2

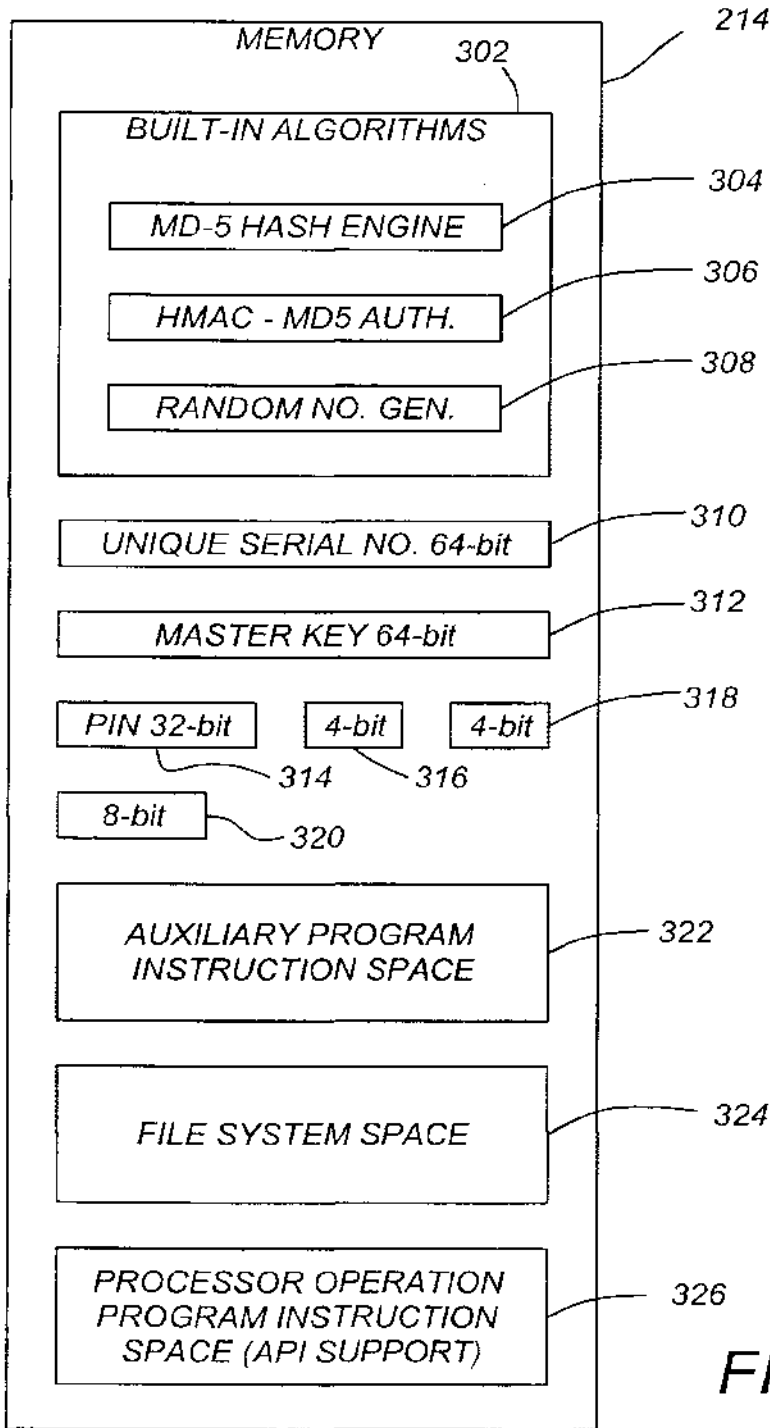


FIG. 3

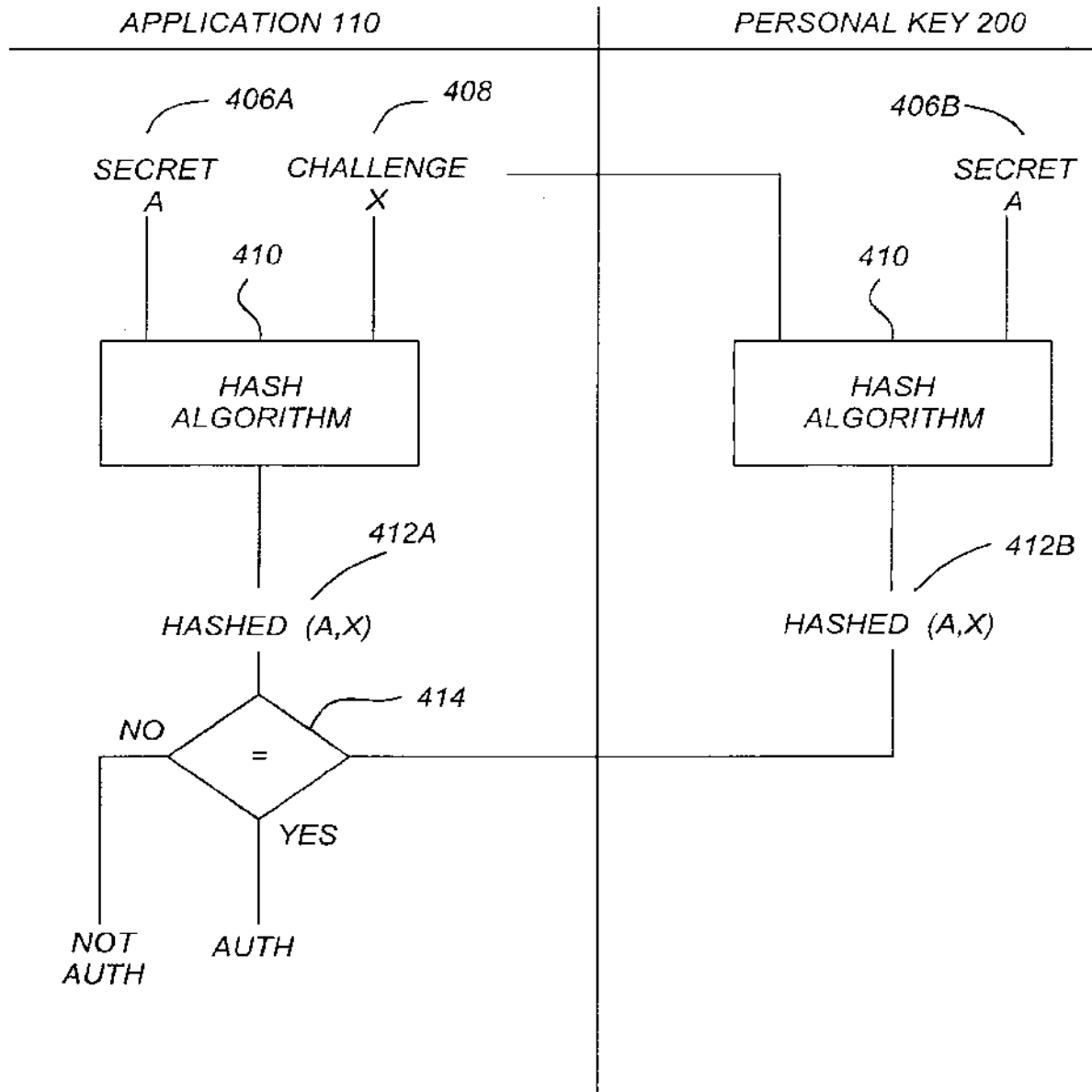
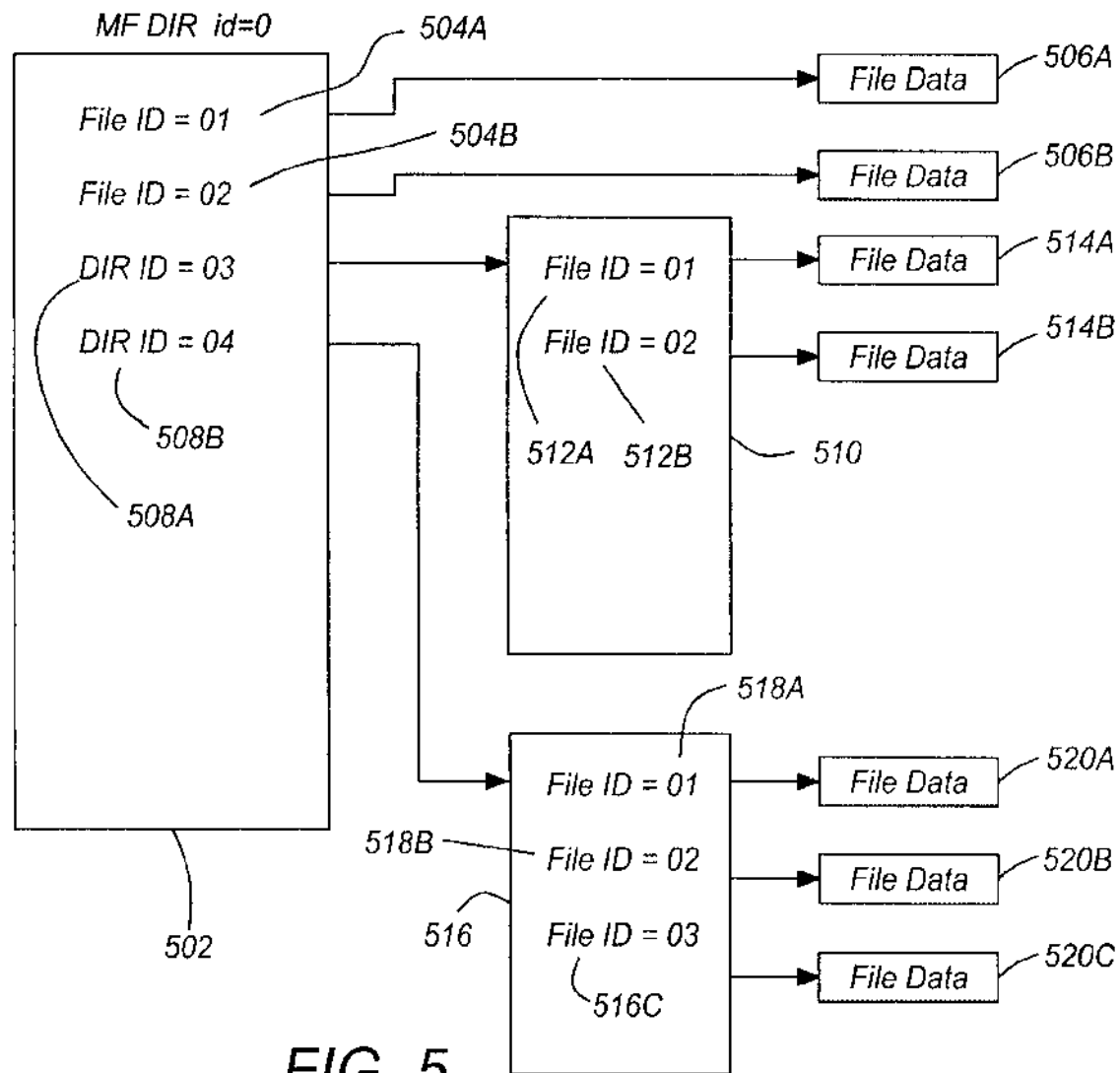


FIG. 4



**FIG. 5**

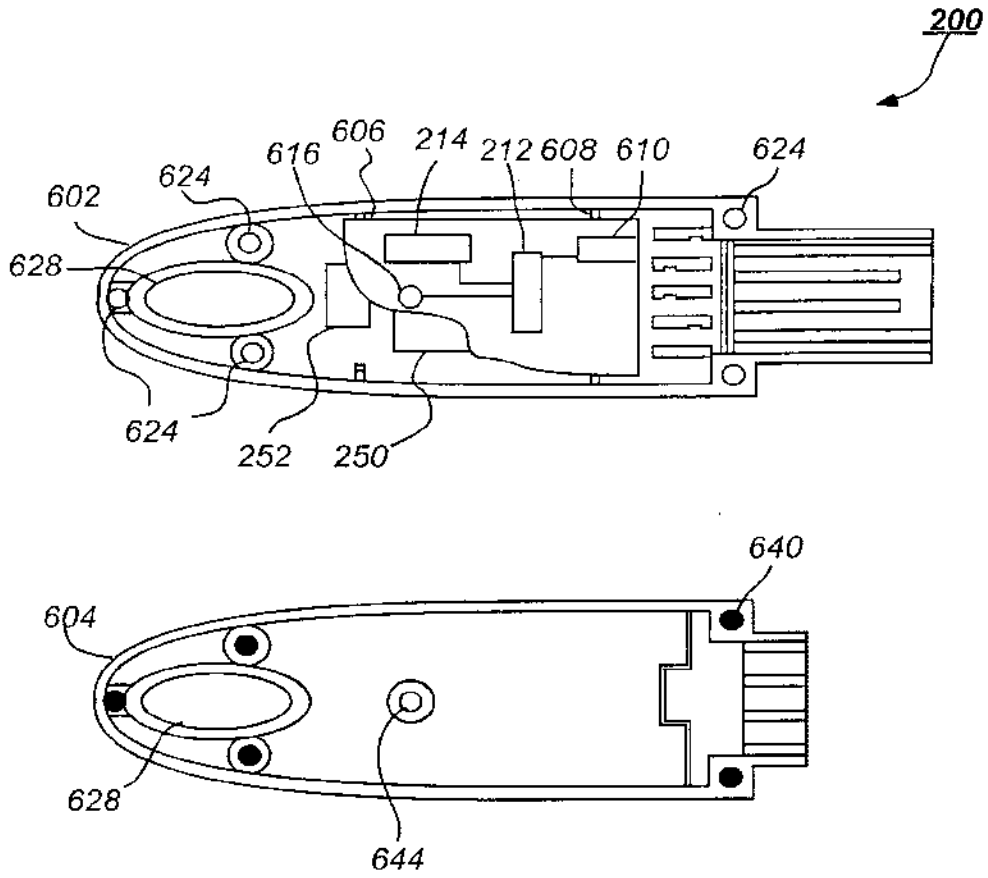
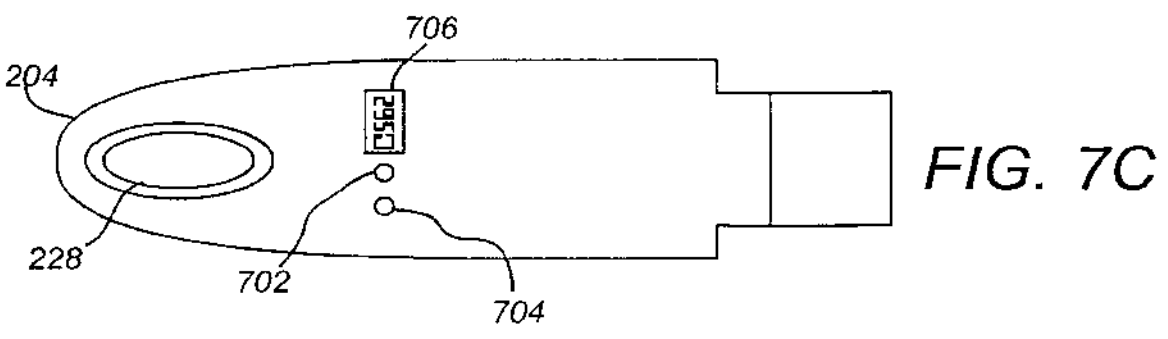
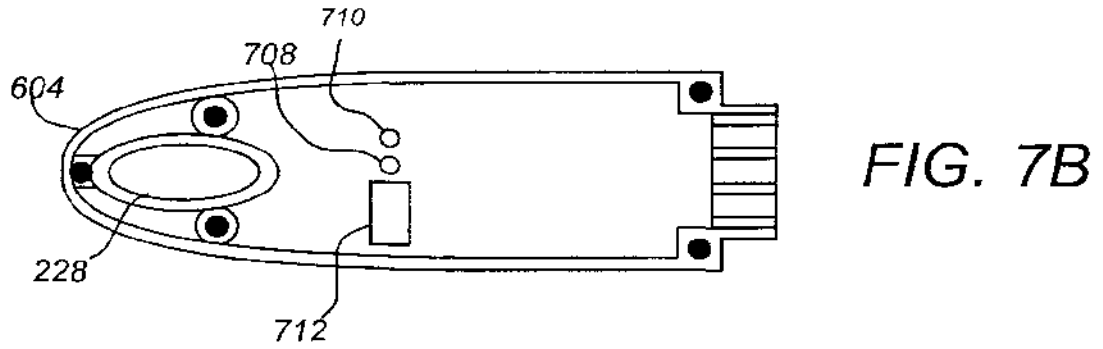
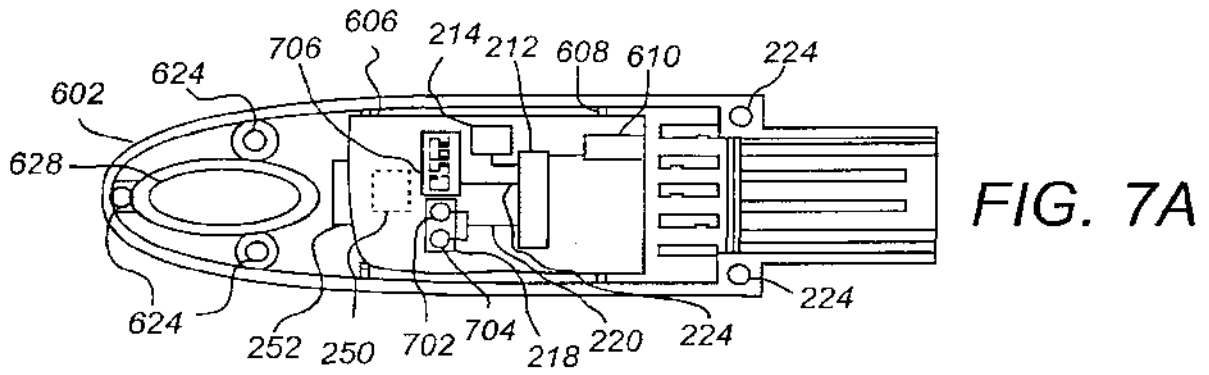


FIG. 6



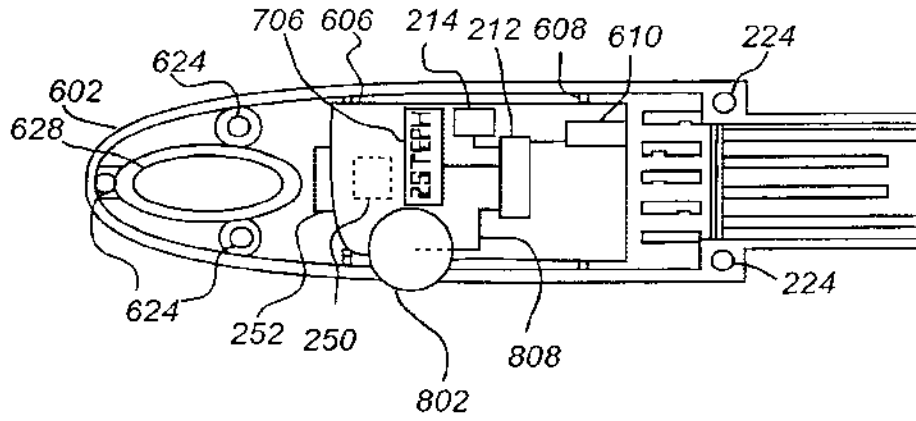


FIG. 8A

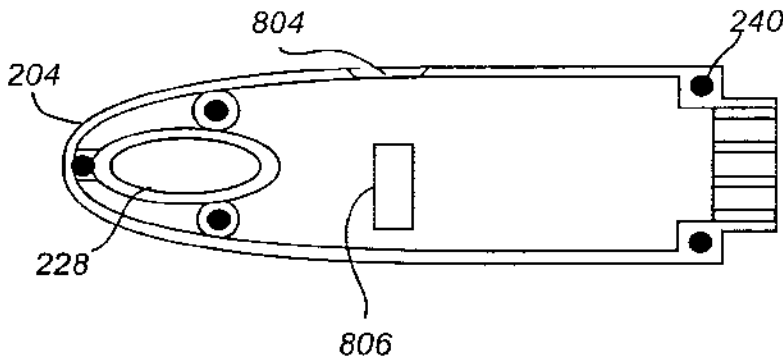


FIG. 8B

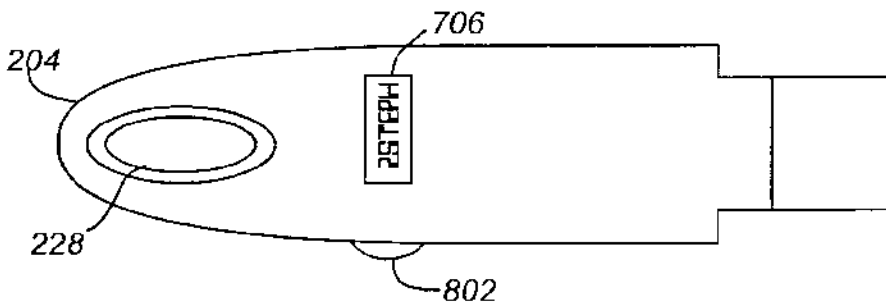


FIG. 8C

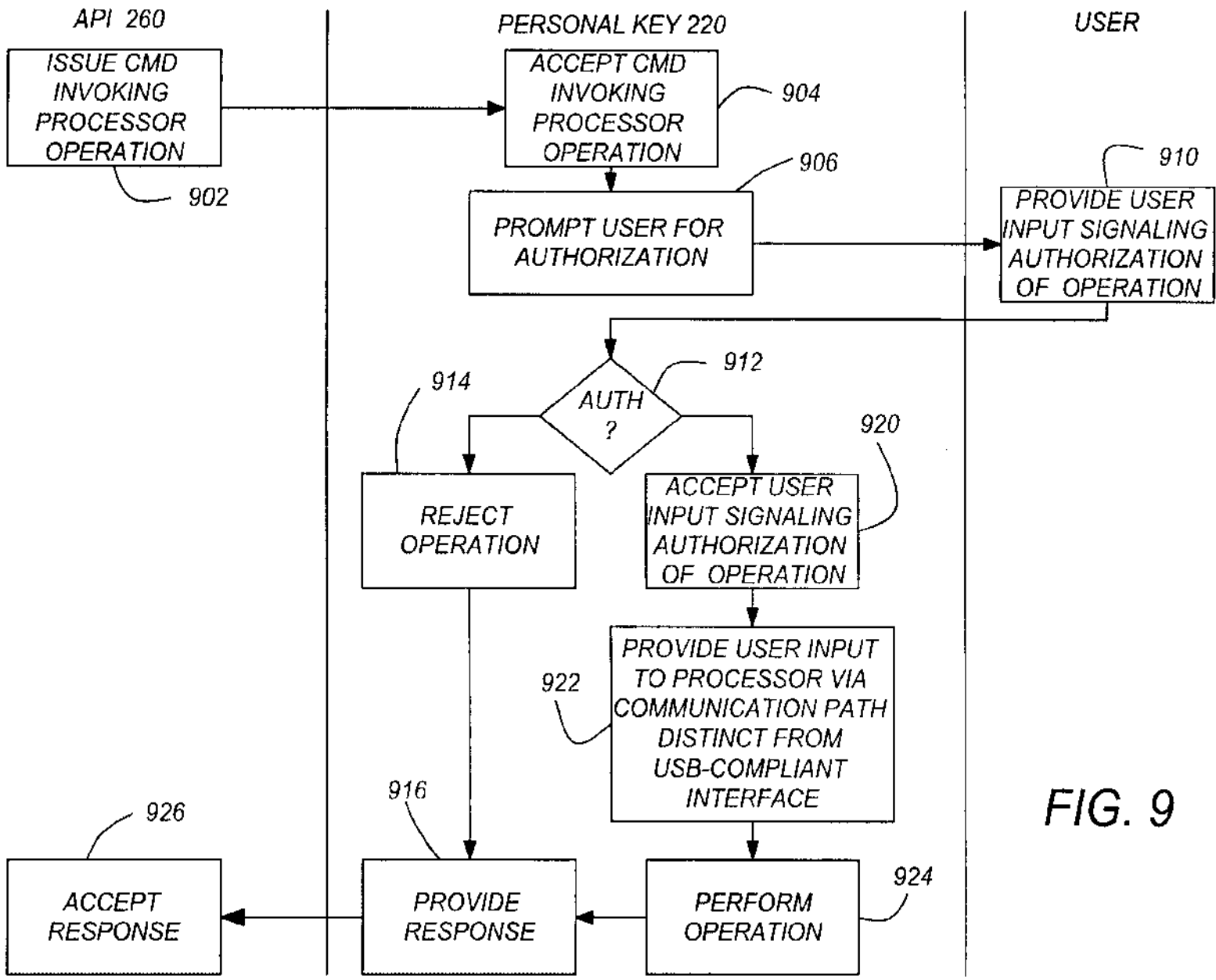


FIG. 9



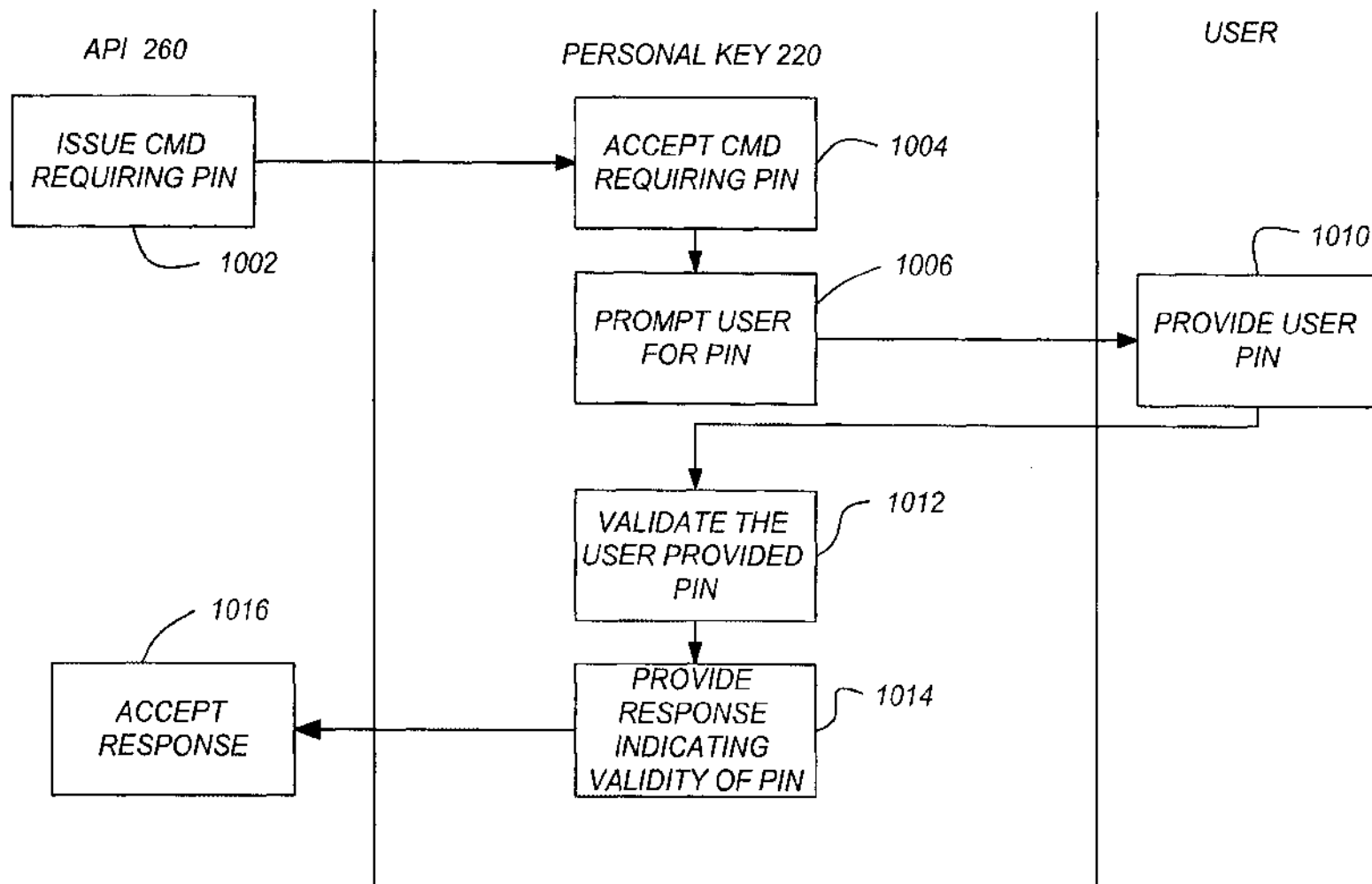


FIG. 10

# INTERNATIONAL SEARCH REPORT

International Application No. PCT/US 00/00711
--

**A. CLASSIFICATION OF SUBJECT MATTER**  
**IPC 7 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 7 G06F**

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.
Y	"WIBU-KEY, User's Guide Version 2.50" 'Online! July 1998 (1998-07), WIBU-SYSTEMS AG, KARLSRUHE, GERMANY XP002139265 Retrieved from the Internet: <URL: ftp://www2.wibu.de/pub/download/us/UG250US .pdf> 'retrieved on 2000-05-25!	1-5,7,9, 11,12, 14-16
A	page 12, paragraph 1 -page 14, paragraph 1 page 164	17
Y	--- GB 2 154 344 A (NAT RES DEV) 4 September 1985 (1985-09-04)  page 3, line 7 - line 62; figures 1-3  --- -/--	1-5,7,9, 11,12, 14-16

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.
- \*Z\* document member of the same patent family

Date of the actual completion of the international search  
31 May 2000

Date of mailing of the international search report  
20/06/2000

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  
Moens, R

INTERNATIONAL SEARCH REPORT

Internatic Application No  
PCT/US 00/00711

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 791 877 A (FRANCE TELECOM) 27 August 1997 (1997-08-27) column 3, line 43 -column 4, line 8; figures ---	1, 3, 4, 11, 12, 14
A	US 5 857 024 A (NISHINO KIYOSHI ET AL) 5 January 1999 (1999-01-05)  column 4, line 6 - line 64; figures 1,7 ---	1, 5-9, 11-13, 15-17
A	"Rainbow Technologies Adds USB Support For PC And Macintosh Software Developers To Sentinel Line" NEWS RELEASE, 'Online! 17 November 1998 (1998-11-17), XP002139273 Retrieved from the Internet: <URL:http://www.rainbow.com/invest/PR98111 7b.html> 'retrieved on 2000-05-28! the whole document -----	1, 3, 4, 11, 12, 14

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/US 00/00711

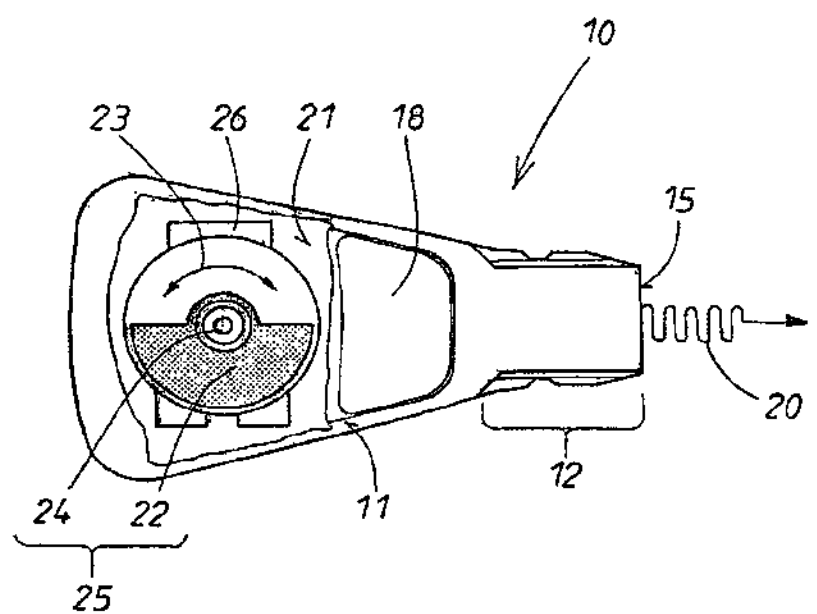
Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2154344 A	04-09-1985	US 4799258 A	17-01-1989
EP 0791877 A	27-08-1997	FR 2745399 A	29-08-1997
US 5857024 A	05-01-1999	JP 9114946 A	02-05-1997

<p>(51) Internationale Patentklassifikation <sup>7</sup> : <b>E05B 49/00</b></p>	<p><b>A1</b></p>	<p>(11) Internationale Veröffentlichungsnummer: <b>WO 00/65180</b></p> <p>(43) Internationales Veröffentlichungsdatum: 2. November 2000 (02.11.00)</p>
<p>(21) Internationales Aktenzeichen: PCT/EP00/02949</p> <p>(22) Internationales Anmeldedatum: 3. April 2000 (03.04.00)</p> <p>(30) Prioritätsdaten: 199 18 817.3 26. April 1999 (26.04.99) DE</p> <p>(71) Anmelder (für alle Bestimmungsstaaten ausser US): HUF HÜLSBECK &amp; FÜRST GMBH &amp; CO. KG [DE/DE]; Steeger Strasse 17, D-42551 Velbert (DE).</p> <p>(72) Erfinder; und (75) Erfinder/Anmelder (nur für US): MÜLLER, Ulrich [DE/DE]; Schneegelskotheln 7C, D-42549 Velbert (DE). VAN DEN BOOM, Andreas [DE/DE]; Mühlenkamp 35, D-45309 Essen (DE). KLEIN, Helmut [DE/DE]; Heidekamp 51, D-42549 Velbert (DE).</p> <p>(74) Anwalt: MENTZEL, Norbert; Kleiner Werth 34, D-42275 Wuppertal (DE).</p>	<p>(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).</p> <p><b>Veröffentlicht</b>  <i>Mit internationalem Recherchenbericht.          Vor Ablauf der für Änderungen der Ansprüche zugelassenen Frist; Veröffentlichung wird wiederholt falls Änderungen eintreffen.</i></p>	

(54) Title: ELECTRONIC KEY, IN PARTICULAR, FOR VEHICLES  
 (54) Bezeichnung: ELEKTRONISCHER SCHLÜSSEL, INSBESONDERE FÜR FAHRZEUGE

(57) Abstract

The invention relates to an electronic key (10), in which coded signals (20) are transmitted and optionally received. In order to achieve this, it is necessary to provide suitable electronic components which are supplied with electric energy by a current reservoir in the housing interior (21). A mass (22) is kinetically mounted (24) in the housing interior (21), in order to ensure that the electronic key (10) is continuously operational. The kinetic energy (23) of said mass (22) which is generated when the key is moved, is converted into electric energy by an electric generator (26), provided in the housing interior (21). The electric energy is subsequently used to continuously recharge the current reservoir.



**(57) Zusammenfassung**

Bei einem elektronischen Schlüssel (10) werden codierte Signale (20) gesendet und gegebenenfalls empfangen. Dazu sind geeignete elektronische Bauteile im Gehäuseinneren (21) notwendig, die von einem Stromspeicher mit elektrischer Energie versorgt werden. Um einen stets betriebsbereiten elektronischen Schlüssel (10) zu gewährleisten, wird vorgeschlagen, eine Masse (22) im Gehäuseinneren (21) beweglich zu lagern (24). Die beim Bewegen des Schlüssels anfallende Bewegungsenergie (23) dieser Masse (22) wird in einem im Gehäuseinneren (21) vorgesehenen elektrischen Generator (26) in elektrische Energie gewandelt, die dann zum dauernden Nachladen des Stromspeichers genutzt wird.

**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	ML	Mali	TR	Türkei
BG	Bulgarien	HU	Ungarn	MN	Mongolei	TT	Trinidad und Tobago
BJ	Benin	IE	Irland	MR	Mauretanien	UA	Ukraine
BR	Brasilien	IL	Israel	MW	Malawi	UG	Uganda
BY	Belarus	IS	Island	MX	Mexiko	US	Vereinigte Staaten von Amerika
CA	Kanada	IT	Italien	NE	Niger	UZ	Usbekistan
CF	Zentralafrikanische Republik	JP	Japan	NL	Niederlande	VN	Vietnam
CG	Kongo	KE	Kenia	NO	Norwegen	YU	Jugoslawien
CH	Schweiz	KG	Kirgisistan	NZ	Neuseeland	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Demokratische Volksrepublik Korea	PL	Polen		
CM	Kamerun	KR	Republik Korea	PT	Portugal		
CN	China	KZ	Kasachstan	RO	Rumänien		
CU	Kuba	LC	St. Lucia	RU	Russische Föderation		
CZ	Tschechische Republik	LI	Liechtenstein	SD	Sudan		
DE	Deutschland	LK	Sri Lanka	SE	Schweden		
DK	Dänemark	LR	Liberia	SG	Singapur		
EE	Estland						

---

## Elektronischer Schlüssel, insbesondere für Fahrzeuge

---

Die Erfindung richtet sich auf einen elektronischen Schlüssel der im Oberbegriff des Anspruches 1 angegebenen Art. Zum Betrieb der elektronischen Bauteile verwendet man in der Regel elektrische Batterien in Form von sogenannten Knopfzellen. Nach einiger Gebrauchszeit entleeren sich die Batterien. Es müssen daher Vorkehrungen getroffen werden, um die Batterien bequem ausbauen, neue Batterien wieder einbauen und zuverlässig kontaktieren zu können. Dafür muss ein geeigneter Platz im Schlüsselgehäuse reserviert sein. Das ist aufwendig. Das Auswechseln der Batterie ist mühevoll und erfordert eine eingehende Belehrung des Schlüsselbesitzers, der dazu nicht immer bereit ist.

Man kann anstelle von solchen Einweg-Batterien auch Akkumulatoren als Stromspeicher für die elektrische Energie im Schlüsselgehäuse verwenden. Es sind aber zum regelmäßigen Aufladen eines solchen Stromspeichers Anschlüsse im Schlüsselgehäuse erforderlich, deren Anordnung wegen der sehr begrenzten Gehäuseoberfläche problematisch ist. Außerdem sind Anzeigemittel für den Ladezustand des Stromspeichers erforderlich, wenn man von einer plötzlichen Entleerung des Stromspeichers nicht überrascht werden will. Auch das erfordert an der Gehäuseoberfläche Platz. Vor allem ist aber während des Ladevorgangs der Schlüssel nicht nutzbar. Der Schlüsselinhaber muss daher die Pausen zwischen der Benutzung des Schlüssels nutzen und die Ladetätigkeit gut einplanen. Das wird als störend empfunden.

Für den Betrieb elektrischer Kleingeräte (DE 196 20 880 A1) ist es bekannt, die zum bestimmungsgemäßen Gebrauch des Geräts erforderliche manuelle Betätigung eines Funktionsauslöseelements dazu zu verwenden, um daraus eine elektrische Energie zu gewinnen. Als Kleingerät verwendete man dabei auch einen mechanischen Schlüssel mit integrierter Infrarot-Sendeeinrichtung. Weil zur Gewinnung der elektrischen Energie ein entsprechendes, mechanisches Energieäquivalent aufgebracht werden muss, ist der Betätiger bei diesem Kleingerät schwergängig. Dies wirkt sich unangenehm bei der Handhabung aus.

Bei einem Türschloss mit einem manuell mittels eines Schlüssels schließbaren Schlossriegel (DE 32 08 818 C2) verwendete man einen elektrischen Antrieb für den Schlossriegel. Der elektrische Antrieb war an einen netzunabhängigen Speicher oder Generator angeschlossen. Die bestimmungsgemäße Betätigung des Schlosses beim Öffnen und Schließen wurde dazu genutzt, um den Generator anzutreiben. Die Betätigung zur Gewinnung elektrischer Energie konnte in einem Fall vom Türgriff ausgehen, der mit dem Generator gekuppelt war. In einem anderen Fall war das Antriebsritzel des dynamischen Generators mit einer Zahnstange eines im Schloss längsverschieblichen Schlüssels verbunden, der beim Ein- bzw. Ausstecken über den Generator elektrische Energie erzeugte.

Schließlich ist es bekannt (DE 197 21 001 C1) bei einem elektronischen Gerät einen längsverschieblichen Schieber oder einen drehbaren Rotationskörper vorzusehen, der, um elektrische Energie für das Gerät zu gewinnen, mit der Hand oder mit den Fingern bewegt werden musste. Die elektrische Energie wurde hier zwar auf mechanischem Wege erzeugt, doch musste dazu der Schieber bzw. der Rotationskörper gezielt manuell angetrieben werden. Das war mühsam und zeitaufwendig. Wurde es vergessen lag keine nutzbare elektrische Energie vor, weshalb der Betrieb des elektronischen Geräts ausfiel. Der Schieber bzw. der Rotationskörper erfordert einen großen Flächenbereich auf der Gehäuseaußenseite, um für die Hand zu Antriebszwecken gut zugänglich zu sein. Die Anwendung auf elektronische Schlösser war zwar vorgesehen, ist aber für elektronische Schlüssel ungeeignet.



Es ist bei Armbanduhren bekannt, dreh- oder schwenkbewegliche Pendel im Uhrengehäuse vorzusehen, welche für die mechanische Energieversorgung des Uhrwerks sorgen. Es liegt aber nicht nahe diese Uhrenmechanik auf elektronische Schlüssel zu übertragen, die, abgesehen von einem eventuellen mechanischen Notschlüssel, keine mechanische Funktionen haben und auf einen elektrischen Stromspeicher angewiesen sind.

Der Erfindung liegt die Aufgabe zugrunde einen preiswerten elektronischen Schlüssel der im Oberbegriff des Anspruches I genannten Art zu entwickeln, dessen Betriebsbereitschaft sich durch einen besonders bequemen Service auszeichnet. Dies wird erfindungsgemäß durch die im Kennzeichen des Anspruches I angeführten Maßnahmen erreicht, denen folgende besondere Bedeutung zukommt.

Die Erfindung hat erkannt, dass der elektronische Schlüssel normalerweise Bewegungen ausgesetzt ist, die sich in Beschleunigungen und Verzögerungen des Schlüssels auswirken. Dadurch werden unvermeidlich dauernd mechanische Kräfte auf den Schlüssel ausgeübt, die zur Gewinnung von mechanischer Energie genutzt werden können. Dies tritt nicht nur in einer Ruhephase des Schlüssels ein, wenn der Schlüssel vom Besitzer in der Hosentasche od. dgl. getragen wird und der Schlüsselbesitzer sich bewegt, sondern auch während der Arbeitsphase des Schlüssels, wenn der Schlüssel im Schloss steckt und das Fahrzeug sich beschleunigend oder verzögernd bewegt.

Ordnet man nun eine Masse im Schlüsselgehäuse beweglich an, so kann die dort anfallende mechanische Energie von einem elektrischen Generator in elektrische Energie gewandelt werden. Diese elektrische Energie kann dann zum Aufladen des im Schlossgehäuse befindlichen Stromspeichers genutzt werden.

Bei der Erfindung ist nicht nur der Stromspeicher sondern auch die Aufladeeinrichtung und die Energieerzeugung im Inneren des Schlüsselgehäuses integriert. Es brauchen daher an der Gehäuseoberfläche keinen besonderen Maßnahmen zur Zugänglichkeit ins Schlüsselinnere oder zur Energieversorgung von

außen erfolgen. Der Schlüsselinhaber braucht sich um die Energieversorgung des elektronischen Schlüssels überhaupt nicht mehr zu kümmern; das Aufladen des Schlüssels erfolgt automatisch bei jeder Schlüsselbewegung, also sowohl in der Ruhe- als auch in der Gebrauchsphase des Schlüssels. Der erfindungsgemäße Schlüssel ist stets betriebsbereit.

Weitere Maßnahmen und Vorteile der Erfindung ergeben sich aus dem Unteranspruch, der nachfolgenden Beschreibung und der Zeichnung. In der Zeichnung ist die Erfindung schematisch in einem Ausführungsbeispiel dargestellt. Es zeigen:

Fig. 1 die Seitenansicht eines elektronischen Schlüssels mit einem Gehäuseausbruch und

Fig. 2 ein Blockschaltbild zur Verdeutlichung des inneren Aufbaus und der Wirkungsweise des erfindungsgemäßen Schlüssels.

Der elektronische Schlüssel 10 umfasst ein Schlüsselgehäuse 11 dessen eines Ende 12 mit einem geeigneten Einsteckprofil 12 versehen ist. Diesem elektronischen Schlüssel ist ein komplementäres elektronisches Schloss zugeordnet, das eine geeignete Aufnahme für das Einsteckprofil 12 aufweist. Im Schlüsselinneren sind verschiedenste elektronische Bauteile 13 vorgesehen, die in definierter Weise miteinander geschaltet sind, z.B. über Leiterbahnen einer sogenannten elektrischen Leiterplatte. Die elektronischen Bauteile 13 haben verschiedene Funktionen zu erfüllen. Außer der Kommunikation mit dem zugehörigen Schloss gehört dazu auch das Aussenden oder Empfangen von codierten Signalen 20, z.B. in Form einer elektromagnetischen hochfrequenten Strahlung. Dazu ist ein geeigneter Sender 14 im Schlüsselgehäuse integriert, zweckmäßigerweise am Stirnende 15 des Einsteckabschnitts 12.

Zur Energieversorgung der Schaltung und ihrer Bauteile 13 dient ein elektrischer Stromspeicher 16. Die elektrischen Bauteile 13 können durch einen Schalter 17

wirksam gesetzt werden. Der Schalter 17 wird von einem Betätiger 18, z.B. einem Taster, ein- und/oder ausgeschaltet. Das ist durch einen Betätigungspfeil 19 im Schema von Fig. 2 veranschaulicht. Dieser Betätiger 18 ist durch eine geeignete Profilierung eines Gehäusebereichs in die Gehäuseschale integriert.

Im Gehäuseinneren 21 ist eine Masse 22 beweglich gelagert, wie durch den Bewegungspfeil 23 veranschaulicht ist. Im vorliegenden Fall ist diese Masse 22 an einem Lagerzapfen 24 frei drehgelagert, weshalb hier ein Pendel 25 vorliegt. Diese Pendelbewegung 25 wird als mechanische Energie einem zugeordneten Generator 26 zugeführt, der elektrische Energie erzeugt und diese über die in Fig. 2 verdeutlichte elektrische Verbindung 27 zum Aufladen des Stromspeichers 16 nutzt.

Die rotatorische Energie eines Pendels 25 ist zwar besonders geeignet, doch wäre es auch möglich, die mechanische Energie durch eine translatorische Bewegung einer Masse 22 zu erzeugen. Die mechanische Energie kann in beliebiger Weise durch bewegliche Massen oder Flüssigkeiten im Inneren des Schlüsselgehäuses erzeugt werden. Entscheidend ist, dass die bei der Benutzung und Nichtbenutzung des Schlüssels anfallenden mechanischen Bewegungen in elektrische Energie umgewandelt werden, die zur Versorgung der elektronischen Bauteile beim bestimmungsgemäßen Gebrauch des elektronischen Schlüssels dient.

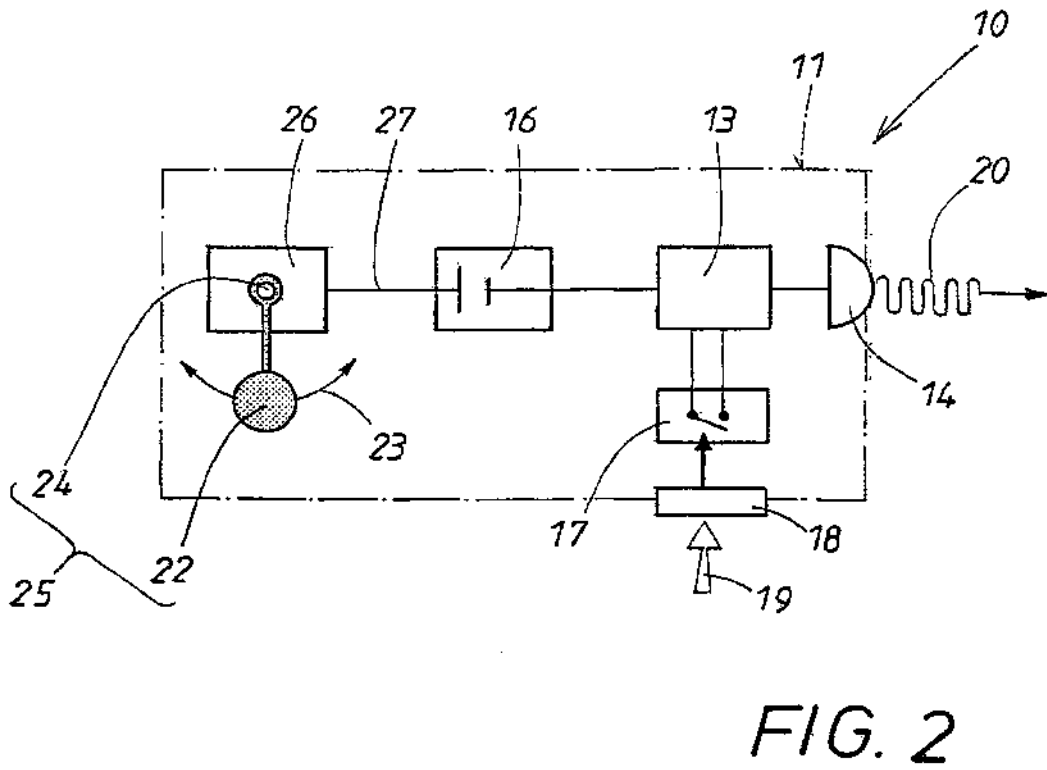
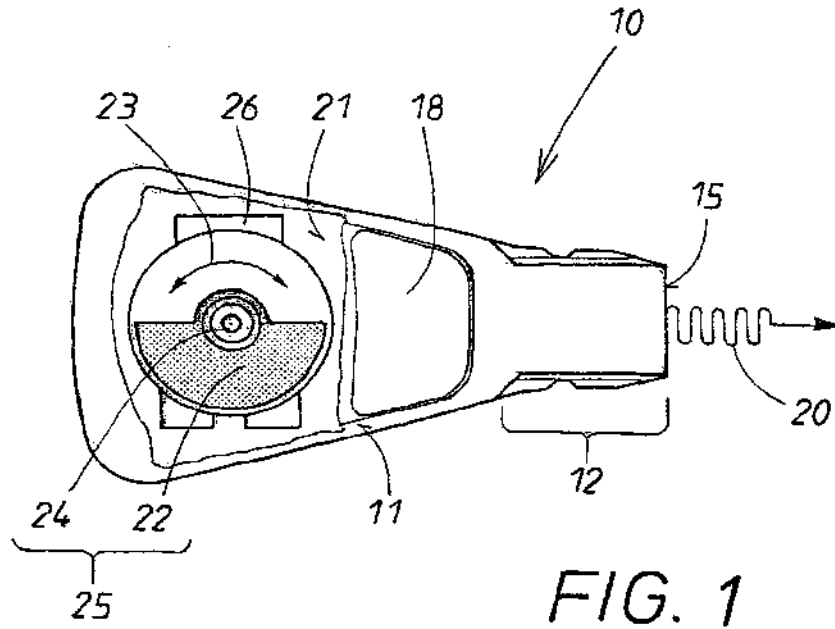
## Bezugszeichenliste :

- 10 elektronischer Schlüssel
- 11 Schlüsselgehäuse von 10
- 12 Einsteckprofil von 11, Einsteckbereich
- 13 elektronische Bauteile in 11
- 14 Sender in 11
- 15 Stirnende von 12
- 16 Stromspeicher in 11
- 17 Schalter
- 18 Betätiger, Taster
- 19 Betätigungspfeil von 18
- 20 codiertes Signal von 14
- 21 Gehäuseinneres von 11
- 22 freibewegliche Masse
- 23 Bewegungspfeil von 22, Pendelbewegung
- 24 Lagerzapfen von 22
- 25 Pendel aus 22, 24
- 26 Generator
- 27 elektrische Verbindung zwischen 26, 16

## P a t e n t a n s p r ü c h e :

- 1.) Elektronischer Schlüssel (10), insbesondere für Fahrzeuge, mit einem Schlüsselgehäuse (11), beinhaltend  
  
einen Sender (14) und gegebenenfalls einen Empfänger für codierte Signale (20) zwecks Kommunikation mit einem zugehörigen elektronischen Schloss,  
  
eine elektrische Schaltung mit elektronischen Bauteilen (13) zur Generierung, zur Codierung und gegebenenfalls zur Decodierung der Signale (20)  
  
und einen Stromspeicher (16) für die zum Betrieb der elektronischen Bauteile (13) benötigte elektrische Energie,  
  
d a d u r c h   g e k e n n z e i c h n e t ,  
  
dass eine bewegliche (23) Masse (22) im Schlüsselgehäuse (11) angeordnet ist und beim Bewegen des Schlüssels mechanische Energie erzeugt,  
  
dass im Schlüsselgehäuse (11) ein Wandler, wie ein elektrischer Generator (26), angeordnet ist, der die mechanische Energie in elektrische Energie wandelt,  
  
und dass die elektrische Energie zum Aufladen des Stromspeichers (16) im Schlüsselgehäuse (11) dient.
- 2.) Schlüssel nach Anspruch 1, dadurch gekennzeichnet, dass die bewegliche Masse (22) aus einem schwenk- bzw. drehgelagerten (24) Pendel (25) besteht.

1 / 1



INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 00/02949

A. CLASSIFICATION OF SUBJECT MATTER  
IPC 7 E05B49/00

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 G04C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, PAJ, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	DE 196 20 880 A (BRANDESTINI) 27 November 1997 (1997-11-27) cited in the application the whole document	1,2
Y	WO 84 01041 A (KNAPEN) 15 March 1984 (1984-03-15) abstract	1,2
A	EP 0 170 303 A (KINETRON BV) 5 February 1986 (1986-02-05) abstract	1,2
A	FR 2 407 599 A (JUILLET) 25 May 1979 (1979-05-25) the whole document	1,2

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.
- \*Z\* document member of the same patent family

Date of the actual completion of the international search

10 August 2000

Date of mailing of the international search report

24/08/2000

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

Van Beurden, J

## INTERNATIONAL SEARCH REPORT

Int. Patent Application No

PCT/EP 00/02949

Patent document cited in search report		Publication date	Patent family member(s)	Publication date
DE 19620880	A	27-11-1997	CN 1219298 A WO 9744883 A EP 0900467 A	09-06-1999 27-11-1997 10-03-1999
WO 8401041	A	15-03-1984	NL 8203443 A AU 1944983 A EP 0119223 A	02-04-1984 29-03-1984 26-09-1984
EP 0170303	A	05-02-1986	NL 8402113 A AT 40223 T DE 3567750 D JP 1612218 C JP 2035547 B JP 61018326 A KR 9005809 B US 4644246 A	03-02-1986 15-02-1989 23-02-1989 30-07-1991 10-08-1990 27-01-1986 11-08-1990 17-02-1987
FR 2407599	A	25-05-1979	NONE	



# INTERNATIONALER RECHERCHENBERICHT

Int. Nationales Aldenzelchen

PCT/EP 00/02949

## A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES

IPK 7 E05B49/00

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

## B. RESEARCHIERTE GEBIETE

Researchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 7 E05B G04C

Researchierte aber nicht zum Mindestprüfstoff gehörende Veröffentlichungen, soweit diese unter die researchierten Gebiete fallen

Während der internationalen Recherche konsultierte elektronische Datenbank (Name der Datenbank und evtl. verwendete Suchbegriffe)

EPO-Internal, PAJ, WPI Data

## C. ALS WESENTLICH ANGESEHENE UNTERLAGEN

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
Y	DE 196 20 880 A (BRANDESTINI) 27. November 1997 (1997-11-27) in der Anmeldung erwähnt das ganze Dokument	1,2
Y	WO 84 01041 A (KNAPEN) 15. März 1984 (1984-03-15) Zusammenfassung	1,2
A	EP 0 170 303 A (KINETRON BV) 5. Februar 1986 (1986-02-05) Zusammenfassung	1,2
A	FR 2 407 599 A (JUILLET) 25. Mai 1979 (1979-05-25) das ganze Dokument	1,2

Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen

Siehe Anhang Patentfamilie

\* Besonders 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

"Z" Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

10. August 2000

Absenddatum des internationalen Recherchenberichts

24/08/2000

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

Van Beurden, J

## INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP 00/02949

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 19620880 A	27-11-1997	CN 1219298 A	09-06-1999
		WO 9744883 A	27-11-1997
		EP 0900467 A	10-03-1999
WO 8401041 A	15-03-1984	NL 8203443 A	02-04-1984
		AU 1944983 A	29-03-1984
		EP 0119223 A	26-09-1984
EP 0170303 A	05-02-1986	NL 8402113 A	03-02-1986
		AT 40223 T	15-02-1989
		DE 3567750 D	23-02-1989
		JP 1612218 C	30-07-1991
		JP 2035547 B	10-08-1990
		JP 61018326 A	27-01-1986
		KR 9005809 B	11-08-1990
US 4644246 A	17-02-1987		
FR 2407599 A	25-05-1979	KEINE	

(19) World Intellectual Property Organization  
International Bureau



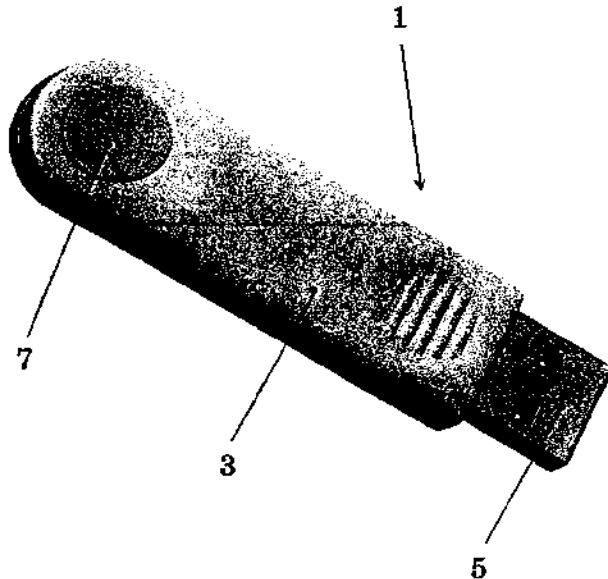
(43) International Publication Date  
14 December 2000 (14.12.2000)

PCT

(10) International Publication Number  
**WO 00/75755 A1**

- (51) International Patent Classification<sup>7</sup>: G06F 1/00
- (21) International Application Number: PCT/IT00/00216
- (22) International Filing Date: 25 May 2000 (25.05.2000)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:  
TO99A000480 8 June 1999 (08.06.1999) IT
- (71) Applicant (for all designated States except US): **EU-TRON INFOSECURITY S.R.L.** [IT/IT]; Via Gandhi, 12, I-24048 Curnasco di Treviso (IT).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): **LEIDI, Michele** [IT/IT]; Eutron Infosecurity S.r.l., Via Gandhi, 12, I-24048 Curnasco di Treviso (IT). **CASSIA, Lucio** [IT/IT]; Eutron Infosecurity S.r.l., Via Gandhi, 12, I-24048 Curnasco di Treviso (IT).
- (74) Agent: **GARAVELLI, Paolo**; A.Bre.Mar. S.r.l., Via Servais, 27, I-10146 Torino (IT).
- (81) Designated States (national): AE, AL, AU, BA, BB, BG, BR, CA, CN, CR, CU, CZ, DM, EE, GD, GE, HR, HU, ID, IL, IN, IS, JP, KP, KR, LC, LK, LR, LT, LV, MA, MG, MK, MN, MX, NO, NZ, PL, RO, SG, SI, SK, TR, TT, UA, US, UZ, VN, YU, ZA.
- (84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), 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 receipt of amendments.
- For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.*

(54) Title: IDENTIFICATION DEVICE FOR AUTHENTICATING A USER



(57) Abstract: A device (1) is described to authenticate a user in an Internet environment, comprising: a support structure (3); a terminal (5) for the connection to a processor port; a microprocessor circuitry to perform safety functions and cryptography algorithms; and activation means (7) to allow enabling an authentication code. A system and a process are further described to input a PIN inside the device (1) and a system and a process to authenticate a user based on such device (1).

WO 00/75755 A1

## IDENTIFICATION DEVICE FOR AUTHENTICATING A USER

The present invention refers to a user authentication system within an Internet architecture based on an hardware device connected to the Universal Serial Bus (USB) port of a client processor through a cryptographic procedure of the "Challenge Response" type. Moreover, the invention refers to a hardware and software system to input a Personal Identification Number (PIN) inside the above-said identification device based on USB port in order to prevent the interception thereof.

With the always wider spreading of the Internet network and other networks of this type, a particular and major importance has been given to problems about the controlled distribution of information on the network, in order to guarantee that these information cannot be attacked and guarantee their privacy as well, in addition to

providing access to particular transactions or information only to authorised users. Several arrangements have so far been proposed, starting from the so-called protecting "hardware keys" to be connected to processors, up to more or less complex cryptographic systems with different types of software keys. The proposed solutions either are very costly to be implemented in terms of several types of resources, or do not guarantee a complete safety of the information to be protected.

Object of the present invention is solving the above prior-art problems, by providing an hardware and software system that is of a reduced cost, easily implemented and absolutely efficient in terms of protection. In particular, the hardware device of the invention is of a simple configuration, has the sizes of a key and, once being inserted into the USB port of a computer, allows univocally recognising and authenticating the user of a network-based application and to start therewith protected and encrypted transactions on the Internet network itself. Authentication uniqueness and transaction safety are based on the features of the device, that is equipped with a microprocessor implemented for

safety functions, and on private-key time-varying cryptographic algorithms.

The above and other objects and advantages of the invention, as will appear from the following description, are obtained by a user authentication device and process as claimed in Claims 1 and 6, respectively, and by a system and process that use the above device as claimed in Claims 15 and 17, respectively. Preferred embodiments and non-trivial variations of the present invention are claimed in the dependent Claims.

The present invention will be better described by some preferred embodiments thereof, given as a non-limiting example, with reference to the enclosed drawings, in which:

- Figure 1 is a perspective view of an embodiment of the device according to the present invention;
- Figure 2 is a block diagram of the architecture of the code-inputting system of the device of the invention;
- Figure 3 is a block diagram of the process realised by the architecture in Fig. 2;
- Figure 4 is a block diagram detailing a step of the process in Fig. 3;

- Figure 5 is a block diagram detailing a step of the process in Fig. 3;
- Figure 6 is a block diagram of the operating process of the device in Fig. 1;
- Figure 7 is a block diagram detailing a step of the process in Fig. 6;
- Figure 8 is a block diagram detailing a step of the process in Fig. 6;
- Figure 9 is a block diagram summarising the steps of the processes in Fig.s 7 and 8; and
- Figure 10 is a block diagram detailing a step of the process in Fig. 6.

With reference to Fig. 1, the device 1 for authenticating a user in an Internet architecture environment substantially comprises an elongated support structure 3, preferably made of plastic material and adapted to be grasped by a user and inserted into a port of a client processor (not shown), for example the Universal Serial Bus (USB) port of a personal computer. For such purpose, the device 1 is equipped with a terminal 5 for the connection to the port and with a microprocessor circuitry contained inside the support structure 3; the circuitry is adapted to perform safety

functions and to operate on cryptographic algorithms. Finally, the device 1 of the invention comprises activation means 7 (commonly realised in the shape of a push-button) supported by the structure 3 and adapted to control the microprocessor circuitry to allow enabling therein an authentication code, as will be described hereinbelow.

In the current and preferred embodiment, the device 1 operates on cryptographic algorithms that are of the private-key time-varying type. Due to the standard interface and "plug&play" USB and to a set of interfacing libraries of the ActiveX and Plug-In type on server and client sides, the device 1 is efficient in terms not only of safety, but also of simplicity and transparency. Its features make it an efficient tool to store keywords, electronic certificates, digital signatures, electronic purse functions or to store and protect therein other interesting information related to user or used services.

With the device 1 of the invention, those who need protecting and checking the access to pages, services, data bases or more generally to areas of Internet sites, will simply have to supply



authorised users of their one Internet service with a suitably initialised device 1. The users will then have to simply insert the device 1 into the USB port of the computer without performing any installation operation. The server application will take care of setting a safe communication with the device 1 in order to authenticate the user. User recognition in fact occurs depending on reserved information inside the device linked with a user keyword. Once having recognised the client and having checked affected user authorisations, the device 1 takes care of sending customised and reserved information to the user, encrypting the contents with an algorithm of the 256-bit Blowfish type, for example, with a time-varying key linked to the secret value contained into the device 1. Information can be indifferently, but not in a limiting way, HTML pages, data bases information with "web" interface, forms, download areas, and the like. The information transaction of the network is performed encrypted both from server to client, and vice versa.

In order to be able to use the above-described device 1, it is necessary to equip it with a univocal Personal Identification Number (PIN) per

user. For such purpose, a system has been implemented whose architecture is shown in Fig. 2, such system being adapted to perform a process as detailed in Figures 3 to 5.

With reference first of all to Fig. 2, the system architecture that allows using the device 1 substantially comprises a processor equipped with a graphic window 10 that displays a digit from 0 to 9. Such window cooperates with a user library 12 (arrow A in Fig. 2), that is a proprietary library that deals with managing the device 1 and, through an identification process 14 contained therein, with checking the enabling of the device 1 itself.

The user library 12 is connected (arrow B in Fig. 2) with a device driver 16, that is also a proprietary library that deals with managing the device 1 at USB level. The device driver 16 is connected (arrow C in Fig. 2) with the device 1 that receives commands (arrow D in Fig. 2) from the push-button 7. According to the flow defined by arrows A to D, in the user library 12 an internal tick pulse is generated so that, upon every tick, a digit is sent both to the window 10 for being displayed, and to the device 1 through the device driver 16; the device driver 16 queries the device

1 whether there are other digits and, if the response is affirmative, goes on with the processing, while otherwise it warns the user library 12 to stop the process. Upon every pressure of the push-button 7, the device 1 stores the currently supplied digit that is also displayed by the window 10.

The general operation of the above-described system is shown as a block diagram in Figs. 3 to 5. Such process guarantees the maximum safety when inputting the PIN to use the device 1. The process first of all comprises, upon request of the PIN code, the activation (301) of the graphic window 10 to display a current digit from 0 to 9.

Then the PIN code is sent (303) for every digit, through a process inserted into the libraries, both to the displaying window 10 and to the device 1.

Upon pressing the push-button 7, therefore, every digit is stored (305) as belonging to the PIN code; then, the process that sends the digit both to the graphic window 10 and to the device 1, queries (307) every time the device 1 to check whether there are other digits: if the response is affirmative, the process goes on by timely sending

(309) the other digits; otherwise, it stops (311) and the final PIN key is stored to validate the device 1.

Upon a more detailed examination, the operation of the PIN code storing step (305) can be divided into two major steps, where the first one deals with managing the display and dispatch of the digits to the device 1, while the second one deals with managing the push-button 7 of the device 1 itself.

In particular, as shown in detail in Fig. 4, the displaying and dispatching step of the digits to the device 1 starts in 401 and comprises the following sub-steps:

- creating (403) the window 10 to display the digits;
- querying (405) whether the digits limit has been reached;
- in case of an affirmative response, removing (407) the displaying window 10; or
- in case of a negative response, sending (409) the digit to the graphic window 10 and to the device 1; and
- requesting (411) to the device 1 whether the

digits limit for the PIN code has been reached, returning to the querying step (405): if the response is affirmative, the process finally ends in 413.

With reference to Fig. 5, instead, the flow diagram of the management step for the push-button 7 of the device 1 is shown in detail, this step being able to be divided into the following sub-steps, starting from the initial one in 501:

- querying (503) whether the digits limit has been reached;
- in case of an affirmative response, ending (509) the process; or
- in case of a negative response, checking (505) whether the push-button 7 has been pressed;
- in case of a negative response, the procedure remains waiting for a following pressure of the push-button 7; or
- in case of an affirmative response, storing (507) the last received digit and returning to the querying step (503) are performed.

After having defined the device 1 of the invention in this way and the system and process to

store and validate the personal code inside the device, it is possible to practice the real and proper process of the invention to manage the accesses to reserved pages and services being present on the Internet network.

As already stated, the system that allows such process is composed, preferably but not in a limiting way, of a central server processor (not shown) that stores and manages the authorised users, connected to a set of local client processors (not shown) equipped with the device 1 of the invention. The detailed procedure is commonly realised through programs being present on both server and client processors, and is shown in Fig.s 7 to 10 of the description.

In particular, with reference to Fig. 6, the process for authenticating a user in an Internet architecture environment comprises the following macro-steps:

- associating (601) a user with an identification device 1;
- identifying (603) the user through the device 1; and
- encrypting (605) information sent/received by/from the user.

In particular, as shown in Fig. 7, the associating step (601) of a user to the device 1 comprises the following sub-steps:

- describing (701) the user;
- generating (703) a TokenId based on describing data of the user;
- performing (705) a first irreversible safe scrambling step (preferably of the MD5 type) of the TokenId after a communication (709) with the server processor managing the keywords;
- creating (706) a first Personal Identification Number (PIN) from the first scrambling (705);
- performing (707) a second irreversible safe scrambling step (preferably of the MD5 + 3DES type) of the TokenId after a communication (709) with the server processor for the keywords;
- creating (708) a second Personal Identification Number (PIN2) from the second scrambling (705), where the second Personal Identification Number (PIN2) is different from the first Personal Identification Number

- (PIN);
- associating the user with an identification string composed of the TokenId, the first Personal Identification Number (PIN) and the second Personal Identification Number (PIN2); and
  - storing such complete identification string into the device 1 and the TokenId alone into a data base on the server processor.

With reference now to Fig. 8 in particular and to Fig. 9 as assembly view of the two steps shown in Figs. 7 and 8, the user identifying step (603) through the device 1 is shown in detail; it comprises the following sub-steps:

- in case of an access by the user to web pages of the network in which an access control must be performed, the server processor sends (801) to the client processor a string of the "Server Challenge" type, that is always different; the string is associated with the first Personal Identification Number (from 706) and is processed by the client to be able to provide a response for the server. For this purpose, the process proceeds with the steps of:



- performing (803) an hashing step (preferably of the MD5 type) on the "Server Challenge" string and the first Personal Identification Number, thereby producing (805) a text string;
- using (807) the second Personal Identification Number (PIN2) (from 708) as encrypting key of a cryptography (809) (preferably of the 3DES type) on the text string;
- generating (811, 813) a string comprising the TokenId and a Response Client and sending such string to the server processor;
- comparing (step 901 in Fig. 9) on the server the received string with the Response Client being generated on the server side by re-processing the first and second Personal Identification Numbers (PIN, PIN2); and
- in case of a positive response to such comparing step (901), pointing out (step 903 in Fig. 9) the existence of a correct identification code; or
- in case of a negative response to such comparing step (901), pointing out (step 905

in Fig. 9) the existence of an incorrect or counterfeited identification code.

Finally, with reference to Fig. 10, the information encrypting step (605) comprises the following sub-steps, performed by the server processor:

- generating (1000) an encryption key from the previous encrypting step (809) by using as input the Server Challenge string and the first and second Personal Identification Numbers (PIN, PIN2);
- receiving (1003) a page from the network;
- encrypting (1001) (preferably using the Blowfish encryption) the received page through the generated encryption key; and
- sending (1005) the encrypted page to the client processor, which, once having received the encrypted pages, is able to decrypt them and reproduce them in a clear way, because it knows both the Server Challenge string and the first and second Personal Identification Numbers (PIN, PIN2).

Some embodiments of the invention have been described, but obviously they are subjected to further modifications and variations within the

same inventive idea. For example, several construction variations of the device 1 will be possible, both from the point of view of the connections to external processor ports, and from the point of view of the internal circuitry to realise the described functionalities. Moreover, the various processes of the invention could be applied to various types of authentication devices, and the systems to realise the described processes could be implemented according to different connection configurations to various types of networks.

**CLAIMS**

1. Device (1) for authenticating a user in an Internet architecture environment, characterised in that the device comprises:
  - a support structure (3);
  - a terminal (5) for the connection to a port of a processor;
  - a microprocessor circuitry contained inside said support structure (3), said circuitry being adapted to perform safety functions and operating on cryptographic algorithms; and
  - activation means (7) supported by said structure (3) and adapted to control said microprocessor circuitry to allow enabling therein an authentication code.
2. Device (1) according to Claim 1, characterised in that said terminal (5) is adapted to be connected to a port of the Universal Serial Bus (USB) type of a personal computer.
3. Device (1) according to Claim 1, characterised in that said activation means (7) are composed of a push-button.

4. Device (1) according to Claim 1, characterised in that said cryptographic algorithms performed by said microprocessor circuitry are of the private-key time-varying type.
5. Device (1) according to Claim 3, characterised in that said cryptographic algorithms are of the "Challenge Response" type.
6. Process for authenticating a user in an Internet architecture environment, characterised in that the process comprises the following steps:
  - associating (601) a user with an identification device (1);
  - identifying (603) said user through said device (1); and
  - encrypting (605) information sent/received by/from said user.
7. Process according to Claim 6, characterised in that said device (1) is the device according to any one of Claims 1 to 5.
8. Process according to Claim 6, characterised in that said associating step (601) comprises the following sub-steps:

- describing (701) said user;
- generating (703) a TokenId based on describing data of said user;
- performing (705) a first irreversible safe scrambling step of said TokenId after a communication (709) with a keywords server processor;
- creating (706) a first Personal Identification Number (PIN) from said first scrambling (705);
- performing (707) a second irreversible safe scrambling step of said TokenId after a communication (709) with a keywords server processor, said second scrambling (707) being different from said first scrambling (705);
- creating (708) a second Personal Identification Number (PIN2) from said second scrambling (705), said second Personal Identification Number (PIN2) being different from said first Personal Identification Number (PIN);
- associating said user with an identification string composed of said TokenId, said first Personal Identification Number (PIN) and said

second Personal Identification Number (PIN2);  
and

- storing said complete identification string into said device (1) and said TokenId into a data base on said server processor.

9. Process according to Claim 8, characterised in that said first scrambling (705) is of the MD5 type and said second scrambling (707) is of the MD5 + 3DES type.

10. Process according to any one of Claims 6 to 9, characterised in that said identifying step (603) comprises the following sub-steps:

- in case of an access by said user to pages of said network in which an access control must be performed, sending (801) by the server processor a string of the "Server Challenge" type, said string being associated with said first Personal Identification Number;
- performing (803) an hashing step on said "Server Challenge" string and said first Personal Identification Number, thereby producing (805) a text string;
- using (807) said second Personal Identification Number (PIN2) as encrypting

- key of a cryptography (809) on said text string;
- generating (811, 813) a string comprising said TokenId and a Response Client and sending said string to said server processor;
  - comparing (901) said received Response Client string with the Response Client being generated on the server side by re-processing said first and second Personal Identification Numbers (PIN, PIN2); and
  - in case of a positive response to said comparing step (901), pointing out (903) the existence of a correct identification code; or
  - in case of a negative response to said comparing step (901), pointing out (905) the existence of an incorrect or counterfeited identification code.
11. Process according to Claim 10, characterised in that said hashing is of the MD5 type and said cryptography (809) is of the 3DES type.
12. Process according to any one of Claims 6 to 11, characterised in that said encrypting step (605) comprises the following sub-steps, performed by said server processor:



- generating (1000) an encryption key from said encrypting step (809) by using as input said Server Challenge string and said first and second Personal Identification Numbers (PIN, PIN2);
- receiving (1003) a page of said network;
- encrypting (1001) said received page through said generated encryption key; and
- sending (1005) said encrypted page to said client processor, said client processor being able to perform the decrypting of said encrypted page depending on said Server Challenge string and said first and second Personal Identification Numbers (PIN, PIN2) being known thereto.

13. Process according to Claim 12, characterised in that said encrypting (1001) is of the Blowfish type.

14. System for authenticating a user in an Internet architecture environment, characterised in that the system comprises:

- at least one central management server processor connected in a network;
- at least one local client processor connected

- in the network;
- at least one authentication device (1) according to any one of Claims 1 to 5 connected to said at least one local client processor; and
  - a control program adapted to perform the process according to any one of Claims 6 to 13.
15. System for inputting a Personal Identification Number (PIN) code inside an identification device (1) in order to prevent intercepting said device (1), characterised in that the system comprises, connected to said device (1), a processor containing:
- at least one user library (12) for managing said device (1), said user library (12) being equipped with an identification process (14) adapted to control the enabling of said device (1);
  - at least one device driver (16) connected to said user library (12), said device driver (16) being a library that manages said device (1) at connection port level; and

- at least one window (10) connected to said user library (12) to display said PIN code digit by digit.
16. System according to Claim 15, characterised in that said device (1) is the device according to any one of Claims 1 to 5.
17. Process for inputting a Personal Identification Number (PIN) code inside an identification device (1) in order to prevent intercepting said device (1), characterised in that the process comprises the following steps:
- upon request of said PIN code, activating (301) a graphic window (10) to display an current digit from 0 to 9;
  - sending (303) every digit of said PIN code both to the displaying window (10) and to the device (1);
  - in case of actuation of activation means (7) of said device (1), storing (305) every digit as belonging to said PIN code;
  - querying (307) said device (1) to check whether other digits exist;
  - in case of an affirmative response to said

querying step (307), timely sending (309) the other digits; or

- in case of a negative response to said querying step (307), stopping (311) the process and storing the final PIN key to validate said device (1).

18. Process according to Claim 17, characterised in that said PIN code storing step (309) comprises the following steps:

- displaying and dispatching the digits to said device (1); and
- managing the activation means (7) of said device (1).

19. Process according to Claim 18, characterised in that said displaying and dispatching step of the digits to said device (1) comprises the following sub-steps:

- creating (403) a window (10) to display the digits;
- querying (405) whether the digits limit has been reached;
- in case of an affirmative response to said querying step (405), removing (407) said displaying window (10); or

- in case of a negative response to said querying step (405), sending (409) the digit to said graphic window (10) and to said device (1); and
  - requesting (411) to said device (1) whether the digits limit for the PIN code has been reached, returning to said querying step (405).
20. Process according to Claim 18, characterised in that said managing step of the activation means (7) of said device (1) comprises the following sub-steps:
- querying (503) whether the digits limit has been reached;
  - in case of an affirmative response to said querying step (503), ending (509) said process; or
  - in case of a negative response to said querying step (503), checking (505) whether said activation means (7) are actuated;
  - in case of a negative response to said checking step (505), suspending the procedure that remains in stand-by; or
  - in case of an affirmative response to said

checking step (505), storing (507) the last received digit and returning to said querying step (503).

21. Process according to Claim 17, characterised in that said device (1) is the device according to any one of Claims 1 to 5.

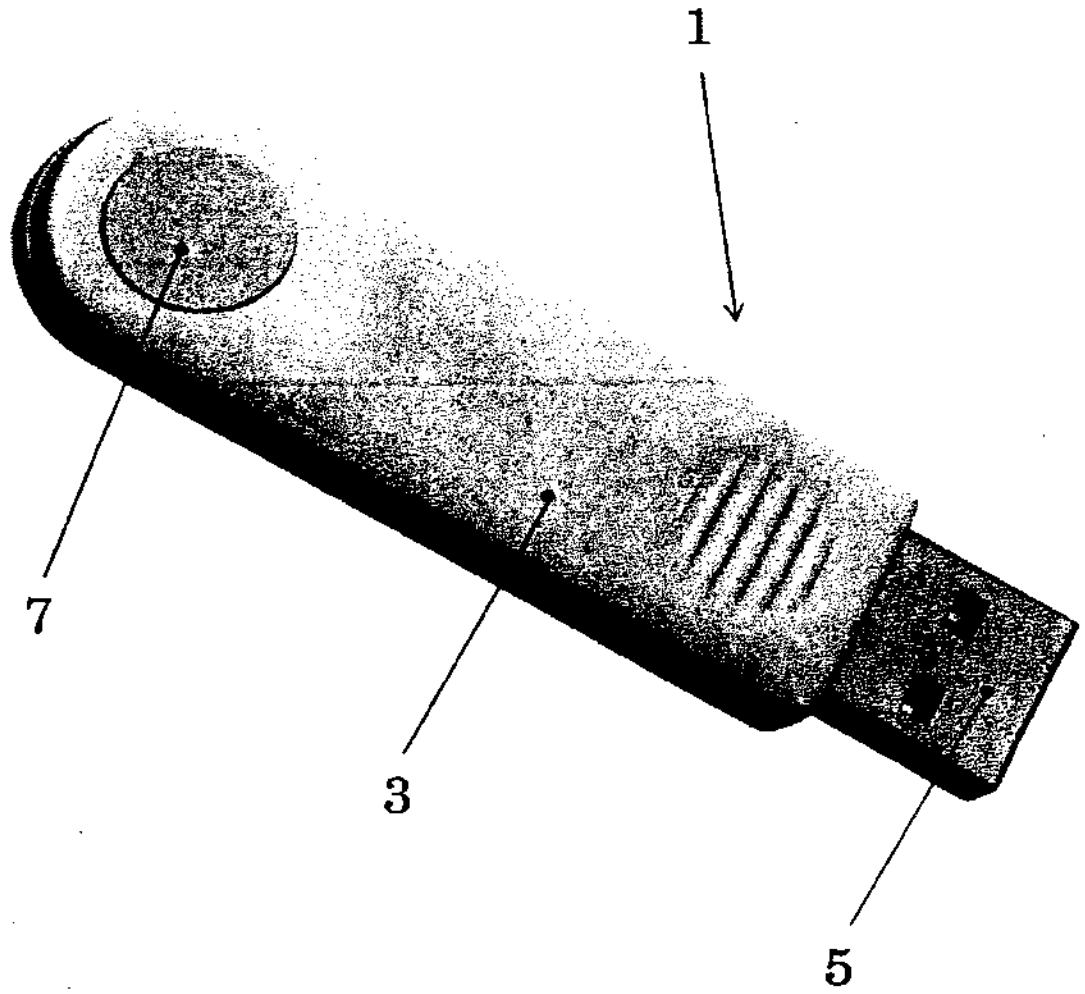


Fig. 1

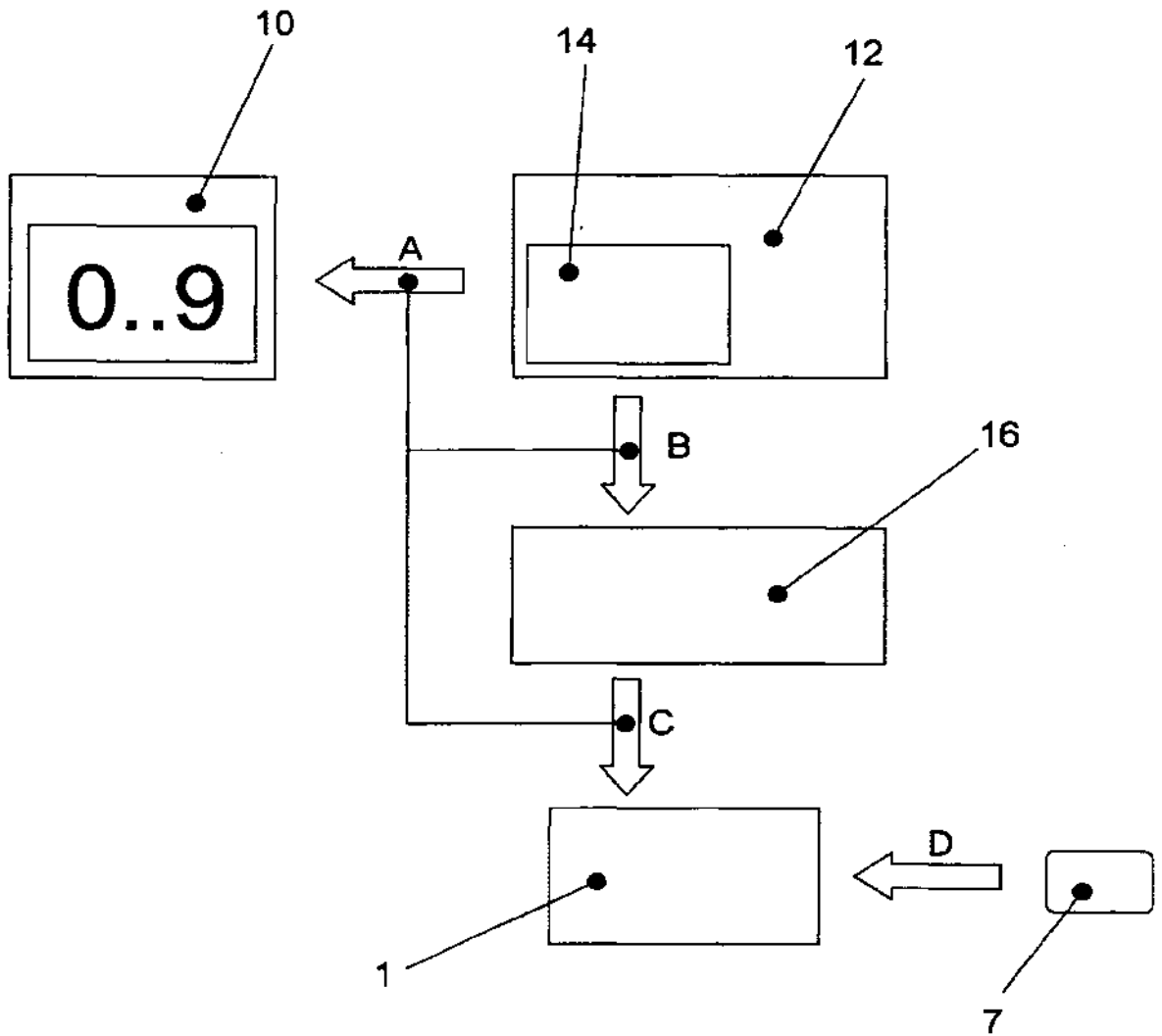


FIG. 2



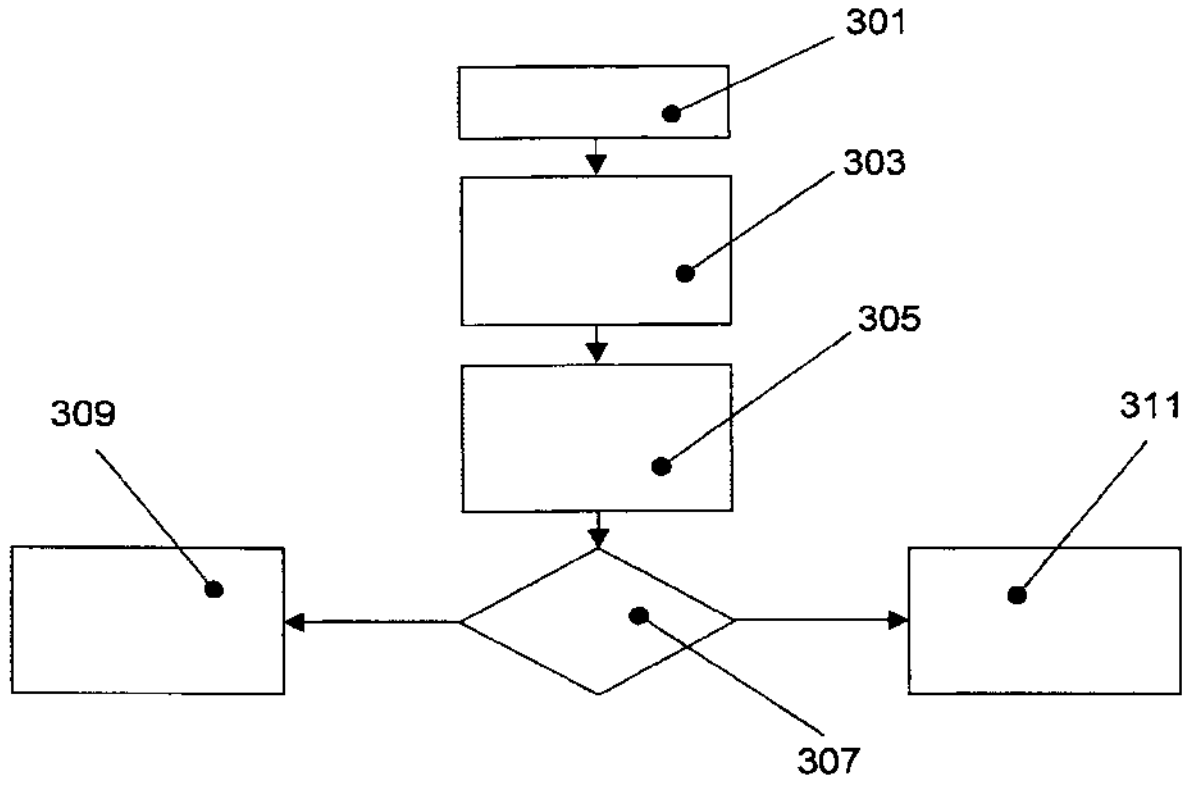


FIG. 3

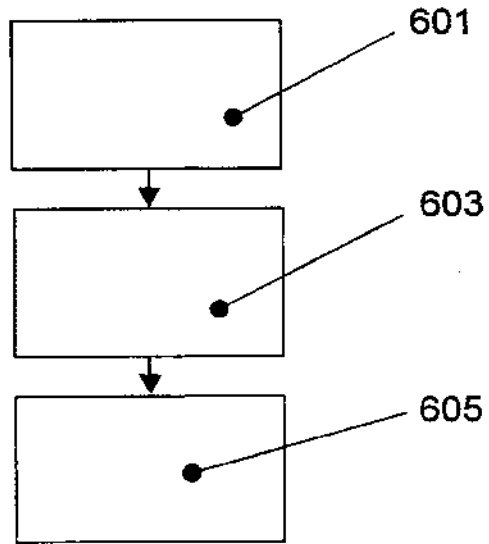


FIG. 6

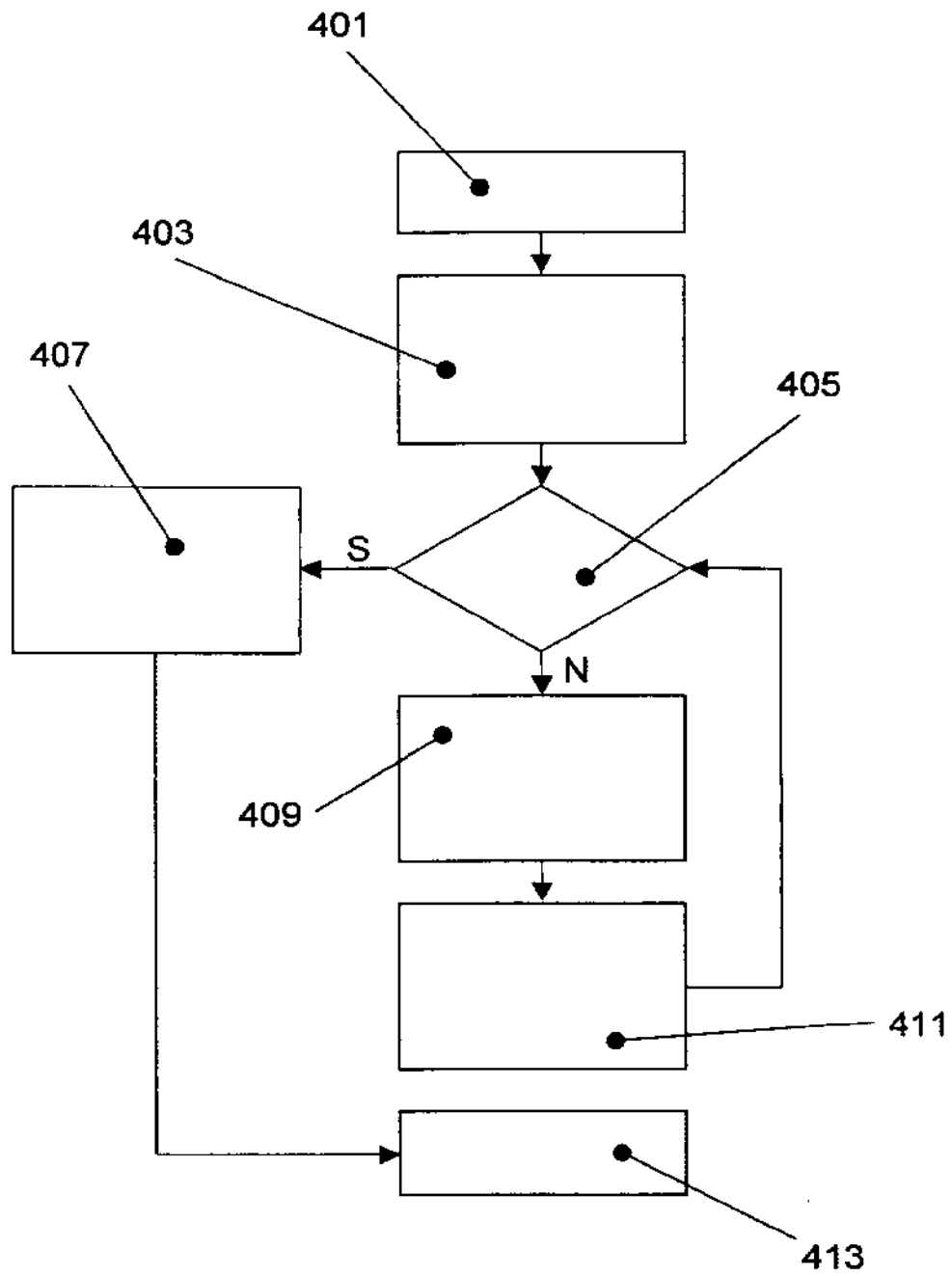


FIG. 4

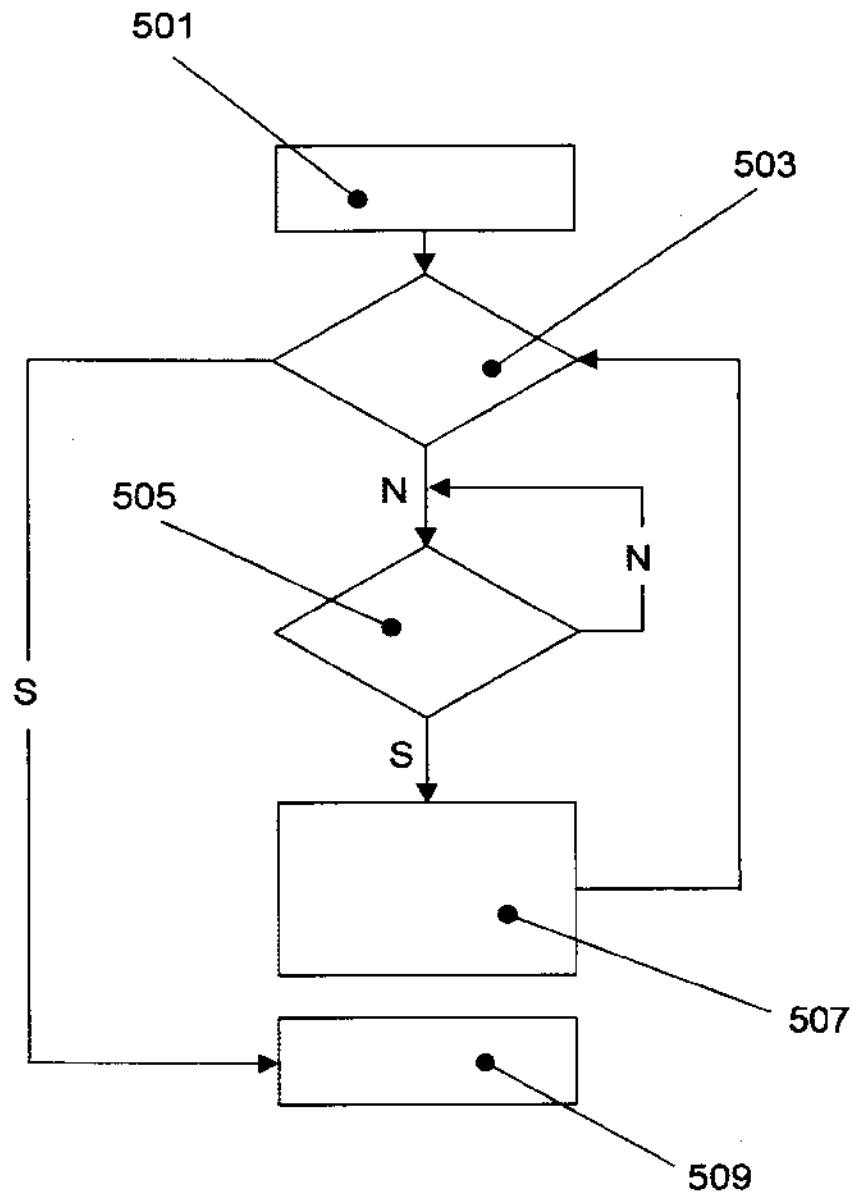


FIG. 5

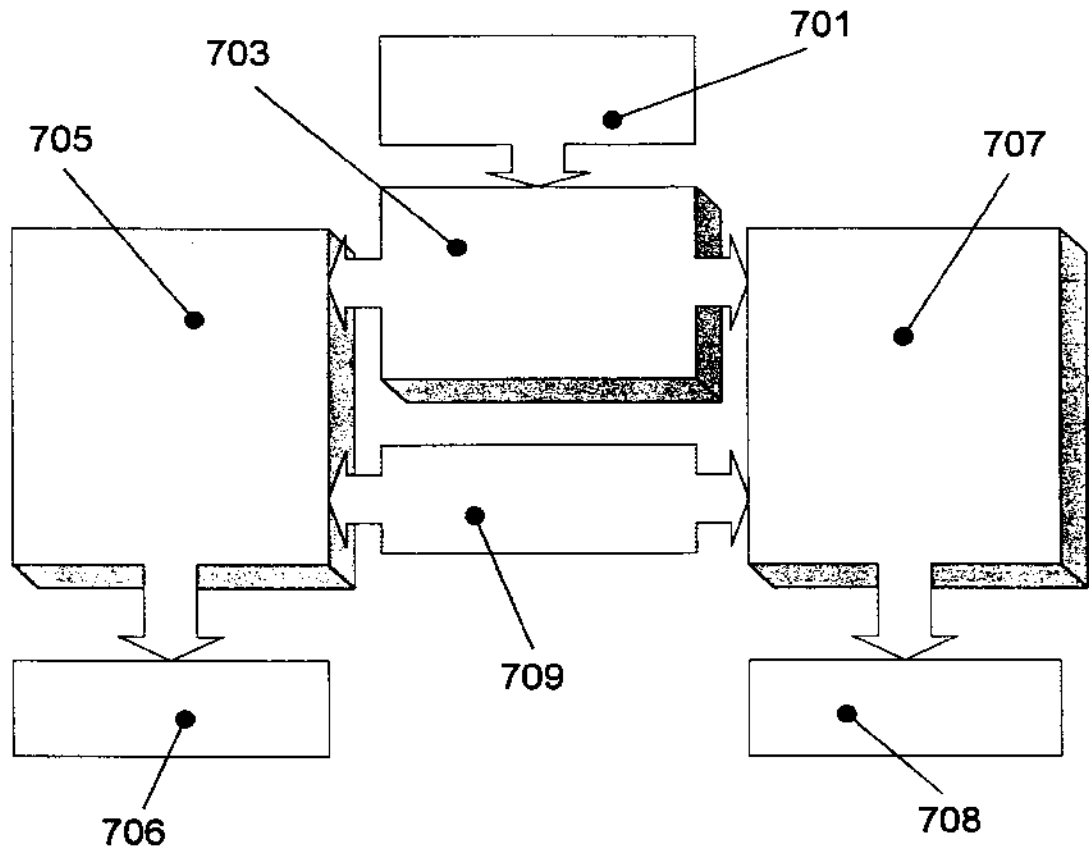


FIG. 7

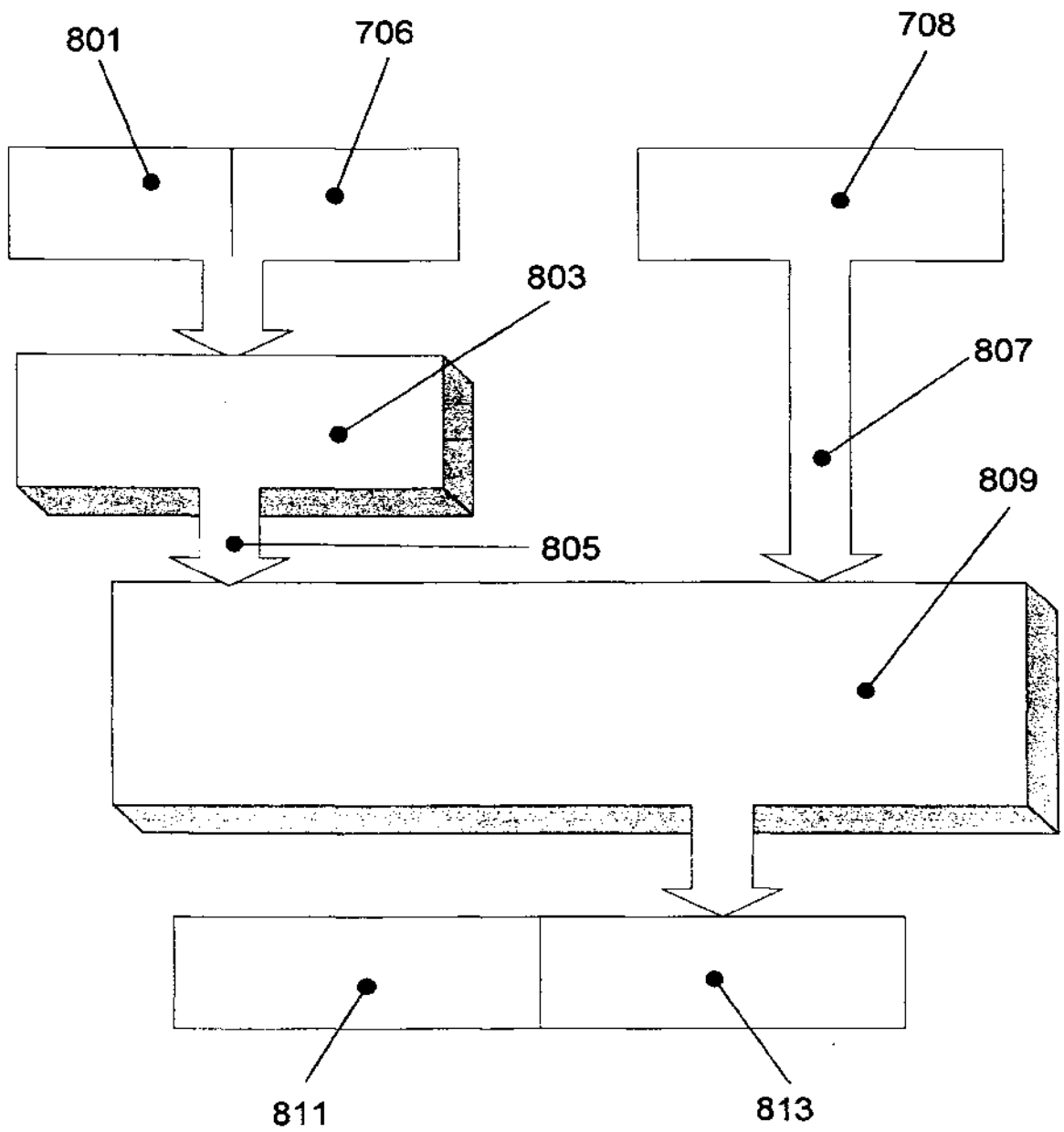


FIG. 8

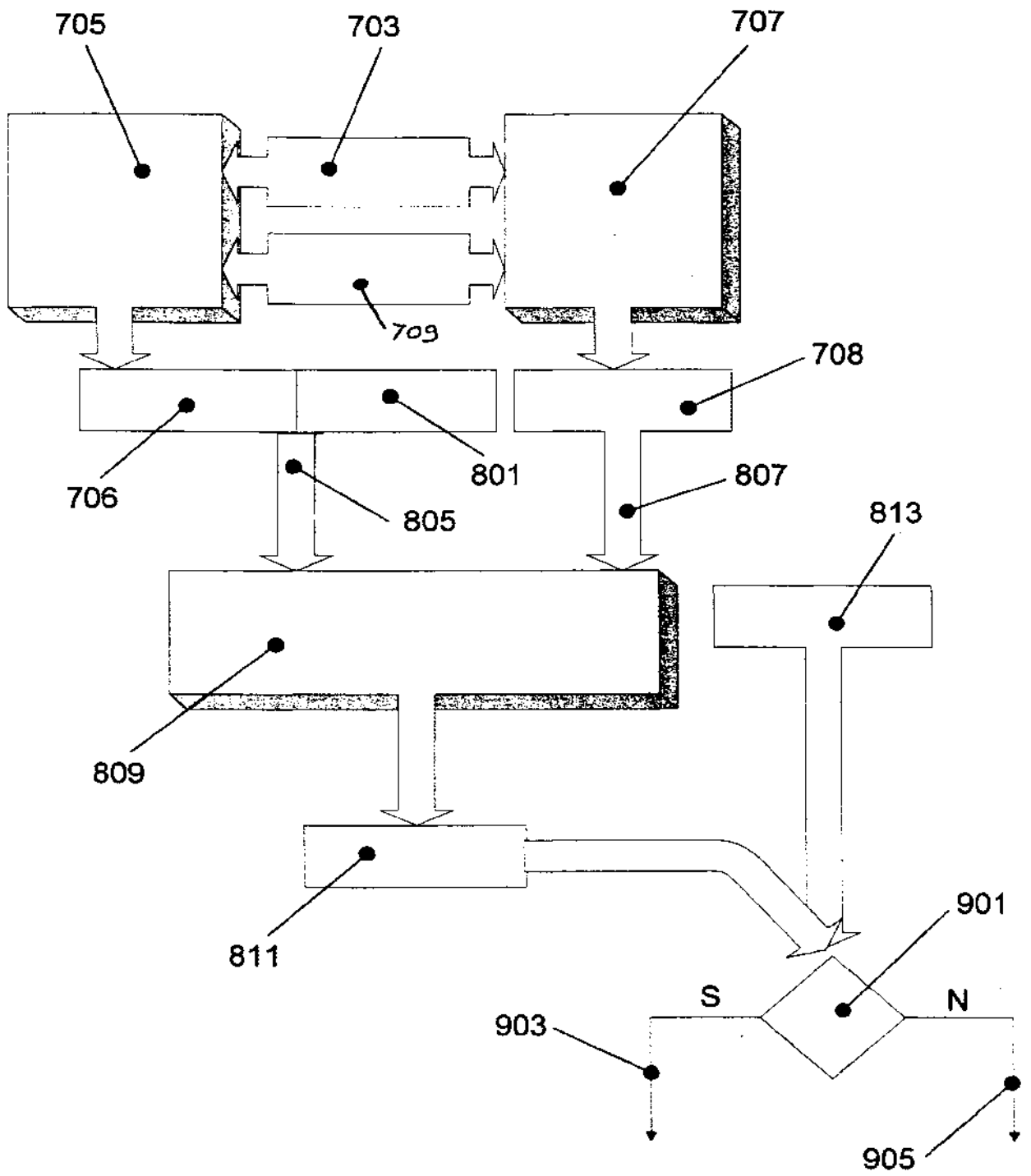


FIG. 9

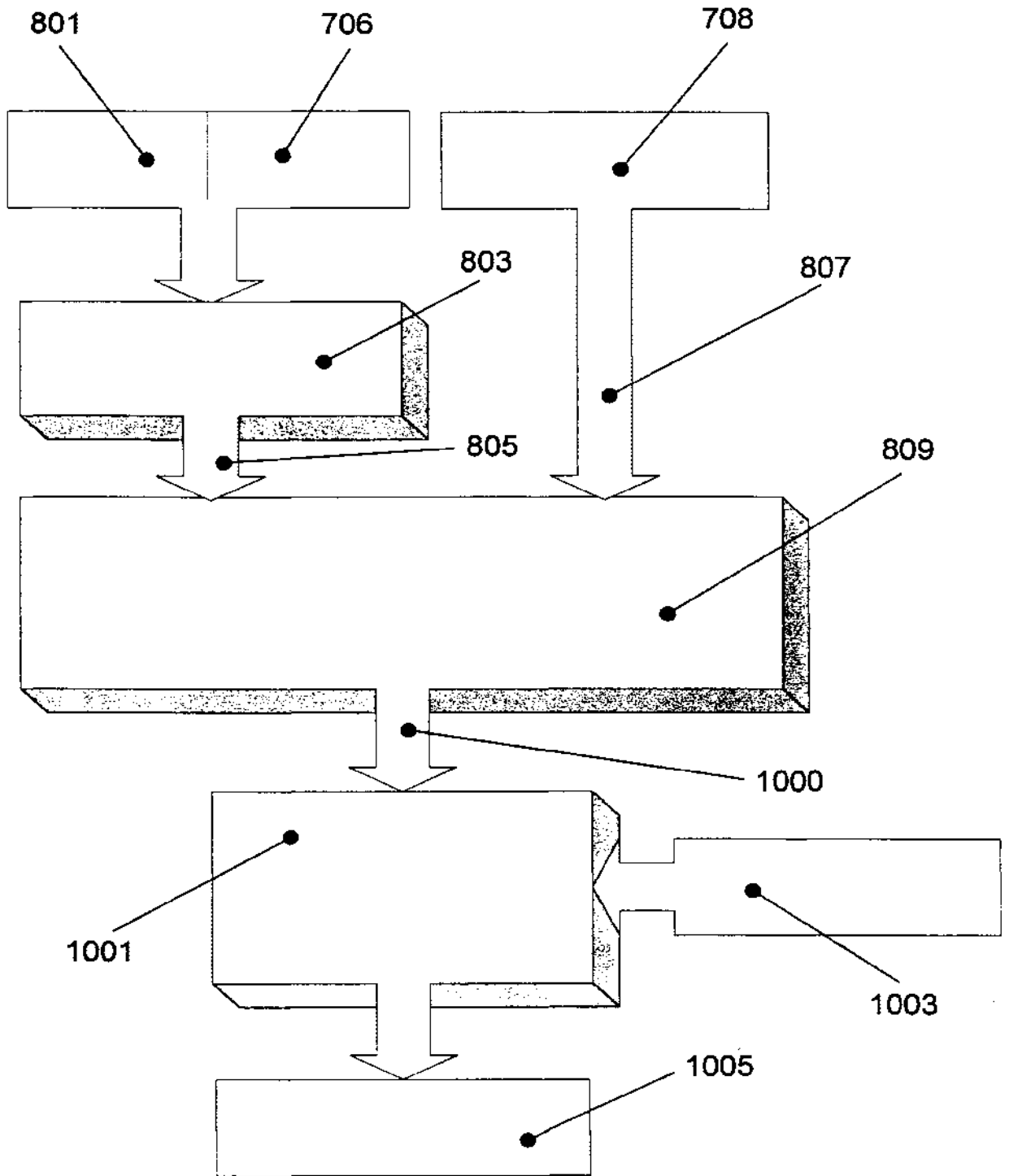


FIG. 10

INTERNATIONAL SEARCH REPORT

Int'l Patent Application No  
PCT/IT 00/00216

<b>A. CLASSIFICATION OF SUBJECT MATTER</b> IPC 7 G06F1/00		
According to International Patent Classification (IPC) or to both national classification and IPC		
<b>B. FIELDS SEARCHED</b> Minimum documentation searched (classification system followed by classification symbols) IPC 7 G06F		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used) EPO-Internal, WPI Data		
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X A	US 5 778 071 A (CAPUTO ET AL) 7 July 1998 (1998-07-07) column 7, line 21 - line 36  column 10, line 51 -column 12, line 22 column 13, line 4 -column 18, line 9; figures 1D,2,4,5-8	1,3-7,14  8-13, 15-21
A	L. PREUSS: "Rainbow Technologies Adds USB Support For PC And Macintosh Software Developers To Sentinel Line" NEWS RELEASE, 17 November 1998 (1998-11-17), XP002139273 the whole document	1,2,4-7, 14,15,17
-/-		
<input checked="" type="checkbox"/> Further documents are listed in the continuation of box C.		
<input checked="" type="checkbox"/> 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  25 October 2000		Date of mailing of the international search report  02/11/2000
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  Moens, R



INTERNATIONAL SEARCH REPORT

International Application No  
PCT/IT 00/00216

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 5 060 263 A (BOSEN ROBERT J ET AL) 22 October 1991 (1991-10-22) column 4, line 6 -column 5, line 24	15, 17
E	WO 00 42491 A (RAINBOW TECHNOLOGIES INC) 20 July 2000 (2000-07-20) page 16, line 16 - line 20; claims 1-3,5,6; figures 7,8	1-5

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/IT 00/00216

Patent document cited in search report	A	Publication date	Patent family member(s)	Publication date
US 5778071	A	07-07-1998	US 5546463 A AU 4147097 A EP 0916210 A WO 9807255 A US 5878142 A	13-08-1996 06-03-1998 19-05-1999 19-02-1998 02-03-1999
US 5060263	A	22-10-1991	NONE	
WO 0042491	A	20-07-2000	NONE	

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum  
Internationales Büro



(43) Internationales Veröffentlichungsdatum  
1. März 2001 (01.03.2001)

PCT

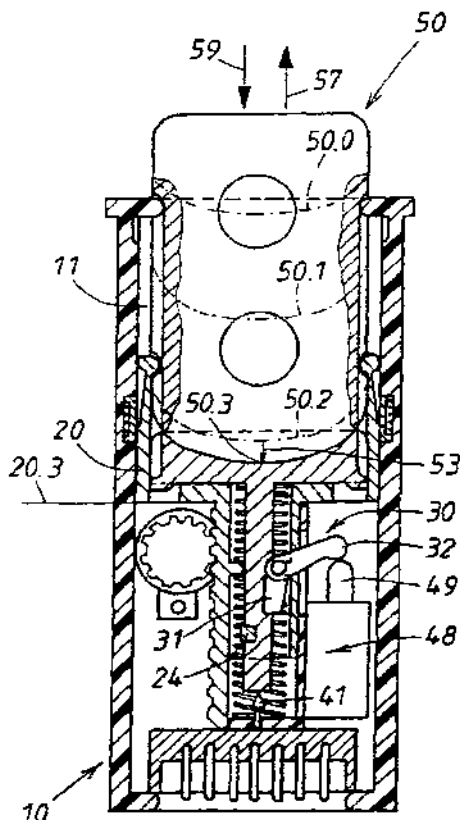
(10) Internationale Veröffentlichungsnummer  
WO 01/14179 A1

- (51) Internationale Patentklassifikation: B60R 25/04 (71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von US): HUF HÜLSBECK & FÜRST GMBH & CO. KG [DE/DE]; Steeger Strasse 17, 42551 Velbert (DE).
- (21) Internationales Aktenzeichen: PCT/EP00/07769 (72) Erfinder; und (75) Erfinder/Anmelder (nur für US): WITTMER, Reinhard [DE/DE]; Beuthener Strasse 26, 42579 Heiligenhaus (DE). BARREBERG, Günter [DE/DE]; Am Buschkothen 20, 42551 Velbert (DE).
- (22) Internationales Anmeldedatum: 10. August 2000 (10.08.2000)
- (25) Einreichungssprache: Deutsch (74) Anwalt: MENTZEL, Norbert; Kleiner Werth 34, 42275 Wuppertal (DE).
- (26) Veröffentlichungssprache: Deutsch (81) Bestimmungsstaaten (national): AU, BR, CN, IN, JP, KR, US.
- (30) Angaben zur Priorität: 199 39 733.3 21. August 1999 (21.08.1999) DE

[Fortsetzung auf der nächsten Seite]

(54) Title: DEVICE FOR STARTING A MOTOR VEHICLE MOTOR, USING AN ELECTRONIC KEY

(54) Bezeichnung: VORRICHTUNG ZUM STARTEN EINES FAHRZEUGMOTORS MITTELS EINES ELEKTRONISCHEN SCHLÜSSELS



(57) Abstract: The invention relates to a device for starting a motor vehicle motor. According to the invention, a slot is (11) used for inserting (59) the key (50) which is usually closed by a spring-loaded cover (14). The key (50) is displaced in the slot (11) into various key positions (20.1), in order to control different functions of the motor or other ancillary devices in the vehicle. In order to ensure a compact construction which is easy to use, the inventive device prevents the key (50) from turning in the slot (11) and the key (50) is displaced into at least three operating positions (20.1) for the control functions which are axially staggered. After being inserted for a first operating distance (51), the key takes up an initial position (20.1), in which it is secured in the slot (11) in a force-fit. In a subsequent second intermediate position, the key (50) is secured in a positive fit which can be locked automatically. This prevents the manual withdrawal (57) of the key (50). In order to remove the key (50), the latter is axially pushed into a third final position, in which the lock on the operating position can be released. During its course of operation, the key (50) is axially spring-tensioned (41) in the direction of the retaining position. The operating position of the key (50) determines the different vehicle functions.

(57) Zusammenfassung: Bei einer Vorrichtung zum Starten eines Motors wird eine Aufnahme (11) zum Einstecken (59) des Schlüssels (50) verwendet, die normalerweise von einer federnden Abdeckung (14) verschlossen ist. Der Schlüssel (50) wird in der Aufnahme (11) in verschiedene Schlüssellagen (20.1) überführt, um verschiedene Funktionen vom Motor oder weiteren Zusatzgeräten im Fahrzeug zu steuern. Um einen platzsparenden Aufbau und

[Fortsetzung auf der nächsten Seite]



WO 01/14179 A1



(84) **Bestimmungsstaaten** (*regional*): europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

- *Mit geänderten Ansprüchen.*

**Veröffentlicht:**

*Mit internationalem Recherchenbericht.*

*Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.*

---

eine einfache Betätigung zu gewährleisten, wird vorgeschlagen, den Schlüssel (50) in der Aufnahme (11) unverdrehbar zu machen und für die Steuerung den Schlüssel (50) in mindestens drei zueinander axial versetzte Hublagen (20.1) zu überführen. Nach einer ersten Hubstrecke (51) des eingeführten Schlüssels kommt der Schlüssel in einer Anfangslage (20.1), wo er in der Aufnahme (11) kraftschlüssig festgehalten wird. Eine formschlüssige Sicherung des Schlüssels (50) ergibt sich in einer dann folgenden zweiten Mittel-lage, welche selbsttätig verriegelbar ist. Dann ist ein manuelles Herausziehen (57) des Schlüssels (50) verhindert. Zur Entnahme des Schlüssels (50) wird dieser in eine dritte Endlage axial eingedrückt, wo die Verriegelung der Betriebslage aufgehoben werden kann. Bei diesen Hubbewegungen ist der Schlüssel (50) in Richtung auf die Haltelage axial federbelastet (41). Die verschiedenen Funktionen des Fahrzeugs werden durch die Hublage des Schlüssels (50) mitbestimmt. (Fig. 5).

Vorrichtung zum Starten eines Fahrzeugmotors mittels eines elektronischen Schlüssels

Die Erfindung richtet sich auf eine Vorrichtung der im Oberbegriff des Anspruches 1 angegebenen Art. Solche Vorrichtungen werden üblicherweise als elektronisches „Zündschloss“ bzw. „Zünd-Lenk-Schloss“ bezeichnet. Mit einem elektronischen Schlüssel wird üblicherweise der Zugang zum Fahrzeug gesichert und entsichert. Dafür sind geeignete Türschlösser vorgesehen. Bei der Verwendung dieses Schlüssel bei der hier interessierenden Vorrichtung wird der Schlüssel in eine im Kraftfahrzeug vorgesehene Aufnahme eingesteckt. In manchen Fällen wird dabei eine dort vorgesehene Abdeckung weggedrückt. Zur Steuerung von verschiedenen Funktionen im Kraftfahrzeug wird der eingesteckte Schlüssel in der Aufnahme in verschiedene Schlüssellagen überführt.

Bei der bekannten Vorrichtung dieser Art (DE 44 34 655 A1) werden die verschiedenen Funktionen durch entsprechende Drehstellungen des elektronischen Schlüssels in der Aufnahme angewählt. Dazu besteht die Aufnahme aus einem Rotor und einem Stator und verschiedenen Sensoren am Stator, welche die verschiedenen Drehstellungen des Rotors zu ermitteln haben. Das ist bau- und platzaufwendig. Um das erforderliche Drehmoment zur Verstellung des Schlüssels manuell ausüben zu können, muss der Schlüssel ausreichend weit aus der Öffnung der Aufnahme herausragen. Ein weit herausragender Schlüssel erhöht aber beim Crashfall des

Fahrzeugs die Verletzungsgefahr. Zusätzlich oder alternativ zur rotatorischen Bewegung kann auch eine translatorische Bewegung des Schlüssels stattfinden.

Bei einer Vorrichtung anderer Art (DE 198 14 964 A1) wird das Fahrberechtigungssignal durch eine Detektion eines Fingerabdrucks der berechtigten Person erzeugt. Dabei wird ein Autorisierungselement in Form einer Scheckkarte verwendet, welche in einen Schlitz neben einem Wippschalter oder in einem Drehschalter eingeführt wird. Der Drehschalter und der Wippschalter besitzen Sensoren für den Fingerabdruck und sind zwischen verschiedenen Schalterlagen druckbetätigbar oder verdrehbar. Dadurch werden verschiedene Funktionen des Motors gesteuert. In diesem Fall sind außer der Einsteckbewegung des Autorisierungselements sowohl eine Drehung oder Druckbewegung eines Schalters als auch die Anbringung eines Fingerabdrucks an der den Sensor aufweisenden Stelle erforderlich. Diese komplexe Betätigung ist umständlich.

Schließlich ist es bekannt, bei einem Startschalter für ein Kraftfahrzeug (DE 195 04 991 C1) in einem Drehgriff einen Schacht zur vollständigen Einführung einer Identifikationskarte vorzusehen. Diese Einführung ist nur in einer ersten Position des Drehgriffs möglich. Von dieser Position ausgehend kann dann der Drehgriff mit der eingesteckten Karte in verschiedene weitere Drehpositionen überführt werden, welche verschiedene Funktionen des Motors steuert. In diesem Fall sind außer den Steckbewegungen auch noch rotative Bewegungen des Drehgriffs erforderlich.

Der Erfindung liegt die Aufgabe zugrunde, eine zuverlässige, bequem betätigbare Vorrichtung der im Oberbegriff des Anspruches 1 genannten Art zu entwickeln, welche die vorerwähnten Nachteile vermeidet. Dies wird erfindungsgemäß durch die im Kennzeichen des Anspruches 1 angeführten Maßnahmen erreicht, denen folgende besondere Bedeutung zukommt.

Bei der Erfindung wird der Schlüssel zur Funktionsauswahl nicht gedreht. Der Schlüssel wird vielmehr beim Einschieben in die Aufnahme in drei zueinander axial versetzte Hublagen überführt, von denen aber für die Zündung des Motors die zweite Hublage maßgeblich ist. In dieser zweiten Hublage ist der Schlüssel nahezu ganz in

der Aufnahme eingeführt. In dieser zweiten Hublage und in der noch tieferen dritten Hublage werden die wesentlichsten Funktionen im Kraftfahrzeug ausgeführt, wofür fallweise weitere manuelle Betätiger oder Pedale genutzt werden. Der Kraftfahrzeugbenutzer braucht nicht am Schlüssel Betätigungen auszuführen, um die gewünschten Funktionen im Fahrzeug auszulösen. Der Schlüssel bleibt vielmehr in der Aufnahme weitgehend versenkt, weshalb im Crashfall keine Verletzungsgefahr durch weit herausragende Schlüsselteile zu befürchten ist.

In seiner zweiten Hublage ist der Schlüssel durch ein Richtgesperre in der Aufnahme fixiert, dessen formschlüssige Haltemittel den Schlüssel gegenüber einer axialen Federkraft sichern. Um den Schlüssel wieder entnehmen zu können, genügt es ihn an seinem Ende anzutippen. Dann wird der Schlüssel in seine dritte Hublage überführt. Das Schlüsselende kann sich dabei beliebig tief in der Aufnahme befinden. In dieser dritten Hublage kann die Verriegelung fallweise freigegeben werden. Dann wird der Schlüssel aufgrund einer auf ihn mittelbar oder unmittelbar einwirkenden axialen Rückstellfederung wieder in seine Anfangslage zurückgedrückt. Dann liegt nur eine kraftschlüssige Verbindung eines Rastgesperres vor. Der Schlüssel kann manuell wieder entnommen werden. Bei der Erfindung sind folglich nur axiale Bewegungen des elektronischen Schlüssels zwischen mindestens drei Hublagen erforderlich, um den Motor oder weitere Zusatzgeräte im Kraftfahrzeug zu steuern. Diese axiale Bewegung ist mit dem Einstecken des Schlüssels in die Aufnahme des Fahrzeugs gleichgerichtet. Es liegt also eine sehr sinnfällige Handhabung des Schlüssels bei der erfindungsgemäßen Vorrichtung vor.

Weitere Maßnahmen und Vorteile der Erfindung ergeben sich aus den Unteransprüchen, der nachfolgenden Beschreibung und den Zeichnungen. In den Zeichnungen ist die Erfindung schematisch in zwei Ausführungsbeispielen dargestellt, von denen jedes der beiden von eigenständiger erfinderischer Bedeutung ist. Das erste Ausführungsbeispiel ist in den Fig. 1 bis 8 und das zweite Ausführungsbeispiel in den Fig. 9 bis 14 veranschaulicht. Es zeigen:

- Fig. 1, einen Axialschnitt durch die Vorrichtung des ersten Ausführungsbeispiels, längs der Schnittlinie I - I von Fig. 3, wobei die Bauteile sich in einer Ausgangsstellung vor dem Einstecken eines zugehörigen elektronischen Schlüssels befinden,
- Fig. 2 die in Fig. 1 gezeigte Vorrichtung in einem demgegenüber rechtwinklig versetzten Axialschnitt, der in Fig. 3 mit II - II gekennzeichnet ist, bei gleicher Stellung der Bauteile,
- Fig. 3 einen Querschnitt durch die Vorrichtung, längs der in Fig. 1 mit III - III gekennzeichneten Schnittlinie,
- Fig. 4 die stirnseitige Draufsicht auf die Vorrichtung von Fig. 1 bis 3,
- Fig. 5, in einer der Fig. 1 entsprechenden Darstellung eine erste Hublage der Bauteile, die sich nach einem anfänglichen Einstecken des elektronischen Schlüssels ergibt,
- Fig. 6 eine durch weiteres axiales Einstecken des Schlüssels in die Aufnahme von Fig. 5 sich ergebende zweite Hublage der Bauteile der in Fig. 1 gezeigten Vorrichtung,
- Fig. 7 eine gegenüber Fig. 6 noch ein wenig tiefer liegende Hublage des eingesteckten Schlüssels, um ihn aus der zweiten Hublage von Fig. 6 in die in Fig. 5 erläuterte erste Hublage zu überführen,
- Fig. 8 die Vorderansicht auf eine im Gehäuse der Vorrichtung vorgesehene Leiterplatte, teilweise im Einbauzustand im Gehäuse,
- Fig. 9 in Analogie zu Fig. 6, einen entsprechenden Axialschnitt durch das zweite Ausführungsbeispiel der erfindungsgemäßen



Vorrichtung, wenn sich der Schlüssel in seiner zweiten Hublage befindet,

Fig. 10 die in Fig. 9 gezeigte zweite Vorrichtung nach der Erfindung bei gleicher Stellung der Bauteile, allerdings in einem gegenüber Fig. 9 rechtwinklig versetzten Axialschnitt durch die Vorrichtung,

Fig. 11 nur einige Bauteile der in Fig. 9 gezeigten Vorrichtung in einer Ausgangsstellung, die sich bei einem aus der Vorrichtung entnommenen Schlüssel ergibt und

Fig. 12-14, in einer der Fig. 11 entsprechenden Darstellung, die Stellung der Bauteile, wenn sich der Schlüssel in drei verschiedenen Hublagen befindet, in Analogie zu den in Fig. 5, 6 und 7 gezeigten Schlüssellagen des ersten Ausführungsbeispiels.

Das in Fig. 1 bis 8 gezeigte erste Ausführungsbeispiel der erfindungsgemäßen Vorrichtung besitzt eine Aufnahme 11 zum Halten eines elektronischen Schlüssels. Die Aufnahme 11 befindet sich im Inneren eines Gehäuses 10. Dieses Gehäuse 10 kann in einer Armatur im Fahrzeuginneren integriert sein, deren Kontur 12 strichpunktiert in Fig. 1 und 2 angedeutet ist. Die Fig. 1 bis 4 zeigen die Vorrichtung bei entnommenen Schlüssel 50. Dann ist die stirnseitige Öffnung 13 der Aufnahme 11 durch eine Abdeckung 14 verschlossen.

Die Abdeckung 14 ist relativ zu einem im Gehäuse 10 vorgesehenen Schieber 20 mit einer leichten Druckfeder 15 belastet und dort zwischen zwei Stellungen, nämlich 14.1 von Fig. 1 und 14.2 axial von Fig. 5 verschieblich. Diese beiden Stellungen 14.1 und 14.2 sind durch einen vorderen und einen hinteren Endanschlag 22, 29 im Schieber 20 bestimmt. Bei entnommenen Schlüssel gemäß Fig. 1 bis 4 liegt die vordere Ausschubstellung 14.1 der Abdeckung 14 vor, wo die Öffnung 13 verschlossen ist. Dann kann Schmutz in das Innere der Aufnahme 11 nicht eindringen. Die Abdeckung 14 befindet sich dann, unter Wirkung ihrer Druckfeder

15 am vorderen Endanschlag 22. Die andere Stellung 14.2 gemäß Fig. 5 wird auf folgende Weise erreicht.

Damit der Schlüssel 50 mit der Vorrichtung zusammenwirken kann, ist eine durch den Pfeil 59 in Fig. 1 und 2 verdeutlichte Einsteckbewegung des Schlüssels 50 in die Aufnahme 11 erforderlich. Dabei kommt der Schlüssel mit der Abdeckung 14 in Berührung. Das ist die strichpunktiert in Fig. 1 und 2 verdeutlichte axiale Lage 50.0. Dabei taucht der Schlüssel mit einem Vorderstück 58 in eine entsprechende Aussparung der Abdeckung 14 bereits ein, welche zu der nachfolgenden Aufnahme 11 im Gehäuse 10 noch hinzukommt. Diese Lage 50.0 des Schlüssels 50 soll nachfolgend kurz „Berührungslage“ bezeichnet werden. Davon ausgehend sollen alle weiteren Hublagen des Schlüssels anhand von Fig. 5 bis 7 beschrieben werden.

Nach einer anfänglichen Einsteckbewegung 59 um eine aus Fig. 5 ersichtliche erste Hubstrecke 51 kommt der Schlüssel in seine in Fig. 5 mit 50.1 gekennzeichnete erste axiale Hublage. Dabei wird, wie bereits erwähnt wurde, die Abdeckung 14 zurückgedrückt und kommt an ihrem zweiten Endanschlag 29 im Inneren des Schiebers 20 zur Anlage. Die Öffnung 13 der Aufnahme ist zwar frei, aber jetzt durch den eingesteckten Schlüssel 50 verschlossen. Die Abdeckung 14 befindet sich dann in ihrer Einschubstellung 14.2. In dieser Hublage 50.1 wird der Schlüssel 50 kraftschlüssig in seiner Aufnahme 11 gehalten wofür die Halteelemente 21, 22, 55 sorgen, deren Aufbau am besten anhand von Fig. 1 zu erkennen ist. Der Schieber 20 ist dosenförmig ausgebildet, wobei die Dosenwand stellenweise eine radial federnde Zunge 21 aufweist, welche ein erstes Halteelement bildet. Diese Zunge 21 ist zunächst ein erster Bestandteil eines zwischen Schlüssel 50 und Schieber 20 bestehenden Rastgesperres. Am Ende der Zunge 21 befindet sich nämlich ein radialer Vorsprung 22, der ein weiteres Halteelement des Rastgesperres darstellt. Dieser Vorsprung 22 kann im Übrigen auch die bereits erwähnten Anschlagfunktionen in der Ausschubstellung 14.1 der Abdeckung 14 erfüllen. Beim Einstecken 59 des Schlüssels 50 führen die Zungen 21 kurzzeitig eine radiale Spreizbewegung aus, bis der an den Zungen 21 sitzende Vorsprung 22 in eine zugeordnete Rastvertiefung 55 am Schlüssel kraftschlüssig eingreift. Das ist in Fig. 5 gegeben. Die Rastvertiefung 55 ist ebenfalls Bestandteil des erwähnten Rastgesperres. Diese erste Hublage 50.1

soll nachfolgend kurz „Anfangslage“ des Schlüssels bezeichnet werden. In dieser Anfangslage 50.1 liegt eine kraftschlüssige Sicherung des Schlüssels in der Aufnahme 11 vor.

Die vorerwähnte Spreizbewegung der Zunge 21 beim Einstecken 59 des Schlüssels ist möglich, obwohl die Zunge 21 auf ihrer dem rastwirksamen Vorsprung 22 gegenüberliegenden Seite einen radialen Gegenvorsprung 23 aufweist. In diesem Bereich besitzt nämlich das Gehäuse 10 eine aus Fig. 1 erkennbare radiale Aussparung 16, in welche dieser Gegenvorsprung 23 beim Schlüsseleinstecken 29 radial ausweichen kann.

Ausweislich der Draufsicht von Fig. 4 ist die Öffnung 13 für die Aufnahme durch eine Blende 17 umgrenzt, die Führungsmittel 18 für den Schlüssel 50 besitzt. Diese bestehen hier aus zwei einander gegenüberliegend angeordneten Stegen 18 an der Blende 17. Die zugehörigen Führungsmittel 54 am Schlüssel bestehen, wie aus Fig. 1 und 2 hervorgeht, aus einer Längsnut. Diese beiseitigen Längsnuten 54 sorgen für ein gutes axiales Einstecken 59 des Schlüssels 50, auch wenn die Außenflächen des Schlüssels aus stilistischen Gründen nicht achsparallel ausgeführt sein sollten. Die vorerwähnte haltewirksame Rastvertiefung 55 ist im Übrigen im Bereich dieser Längsnut 54 angeordnet. Der in seine Anfangslage 50.1 von Fig. 5 befindliche Schlüssel 50 kann von Hand wieder im Sinne des Pfeils 57 von Fig. 5 manuell herausgezogen werden. Dann fährt die Abdeckung 14 wieder in ihre Ausschubstellung 40.1 von Fig. 1 zurück. Der Schlüssel kann auch in einer um 180 ° gewendeten Position eingesteckt werden.

Das Herausziehen 57 des Schlüssels ist aber verhindert, wenn der Schlüssel, ausgehend von seiner Anfangslage 50.1 von Fig. 5 um eine weitere, beträchtliche Hubstrecke 52 bis zu seiner in Fig. 6 erkennbaren zweiten axialen Hublage 50.2 überführt worden ist. Dann ist nämlich der Schlüssel 50 sogar formschlüssig in der Aufnahme 11 gesichert. An diesem Formschluss sind zunächst die gleichen Halteelemente 21, 22, 55 wie beim Rastgesperre beteiligt, das vorausgehend für den kraftschlüssigen Zusammenhalt zwischen dem Schieber 20 und dem Schlüssel 50 sorgte. Der an der federnden Zunge 21 vom Schieber 20 vorgesehene

Gegenvorsprung 23 kommt in diese Hublage 50.2 an einer aus Fig. 6 erkennbaren radialen Stützfläche 19 im Gehäuse 10 zu liegen. Diese Stützfläche 19 befindet sich unterhalb der vorausgehend in der Anfangslage 50.1 damit ausgerichteten radialen Aussparung 16. In seiner Hublage 50.2 wird also der Schlüssel 50 in der Aufnahme 14 formschlüssig verriegelt. Ein Herausziehen 57 im Sinne des auch in Fig. 6 eingezeichneten Pfeils ist nicht möglich. Diese zweite Hublage 50.2 des Schlüssels soll nachfolgend kurz „Mittellage“ bezeichnet werden.

Die axiale Position des Schiebers 20 von Fig. 5 oder 6 wird durch eine weitere Einsteckbewegungen 59 des Schlüssels 50 erreicht. In Fig. 5 befindet sich der Schieber 20 in einer dort mit 20.1 gekennzeichneten Ausgangsposition, welche die äußere Position des Schiebers im Gehäuse 10 ist. Diese Ausgangsposition 20.1 liegt im Übrigen auch in Fig. 1 bzw. Fig. 2 vor, wo der Schlüssel 50 ganz entfernt ist oder mit der Abdeckung 14 in Berührung 50.0 kommt. Die vorgenommene Hublage 50.2 des Schlüssels 50 ist zunächst gesichert, weil der den Schlüssel 50 aufnehmende Schieber 20 in der zugehörigen Axialposition 20.2 verriegelt wird. Dafür dient ein hier als federnde Klinke 30 ausgebildeter Riegel, der einen Sperrarm 31 und einen damit drehfesten Stellarm 32 aufweist. Der Riegel 30 ist bei 33 ortsfest im Gehäuse 10 schwenkbar gelagert und greift mit seinem Sperrarm 31 in den Betätigungsweg einer Schulter 24, die beim Axialbewegen des Schiebers 20 mitbewegt wird. Die Schulter 24 befindet sich hier an einem Nocken, der Bestandteil eines aus Fig. 5 erkennbaren Axialansatzes 25 des Schiebers 20 ist. Der Axialansatz 25 taucht beim Bewegen des Schiebers 20 entlang der Hubstrecke 52 teleskopartig in eine gehäusefeste Hülse 45 ein.

Die Gehäusehülse 45 und der Axialansatz 25 dienen im Übrigen auch zur Aufnahme einer kräftigen Rückstellfeder 40, die bestrebt ist, den Schieber 20 in dessen Ausgangsposition 20.1 zu halten. Dazu ist zweckmäßigerweise auch der Axialansatz 25 vom Schieber 20 rohrförmig ausgebildet und besitzt einen Innenbund 26 an dem sich das obere Ende der Rückstellfeder 40 abstützt. Der obere Bereich dieses rohrförmigen Axialansatzes 25 kann seinerseits als Aufnahme für die bereits oben beschriebene Abdeck-Druckfeder 15 dienen, die demgegenüber sehr viel weicher ausgebildet ist. Die Rückstellfeder 40 übt auf den Schieber 20 eine durch den Pfeil

41 in Fig. 5 verdeutlichte Rückstellkraft aus. Dadurch wird der Schieber 20 gegen einen gehäusefesten Endanschlag 42 gedrückt, der hier durch die Innenfläche der beschriebenen Blende 17 gebildet wird. Dieser Anschlag 42 bestimmt die Ausgangsposition 20.1 des Schiebers 20. Der Nocken mit der Schulter 24 befindet sich in der Ausgangsposition 20.1 des Schiebers 20 noch axial oberhalb der Klinke 30.

Die Schulter 24 wirkt mit der Klinke 30 nach Art eines sogenannten „Richtgesperres“ zusammen. Der Sperrarm 31 befindet sich mit seinem Sperrende in dem durch eine Punktlinie 27 in Fig. 5 veranschaulichten Verschiebungsweg 27 der Schulter 24. Bei der Einsteckbewegung 59 von Fig. 5 fährt der die Schulter 24 tragende Nocken gegen den Sperrarm 31 der Klinke 30 und drückt diese weg, bis die Schulter 24 in ihrer aus Fig. 6 ersichtliche Position gekommen ist. Dann schnappt der Sperrarm 31 vor die Schulter 24 und hält den Schieber 20 gegen die axiale Federbelastung 41 in der Axialposition 20.2 fest. Eine Rückbewegung des Schiebers 20 in die vorausgehende Axialposition 20.1 ist zunächst nicht möglich.

Die der Mittellage 50.2 des Schlüssels 50 von Fig. 6 entsprechende Axialposition 20.2 des Schiebers 20 soll als „Arbeitsposition“ bezeichnet werden. In dieser Mittellage 50.2 erkennt zunächst eine elektronische Steuereinheit der Vorrichtung z.B. auf elektrischem oder elektromagnetischem Weg, dass es sich um den richtigen Schlüssel 50 handelt. Als Identifikationsmittel dient im vorliegenden Fall ein im Gehäuse 10 integrierter Transponder 43, der Bestandteil der nicht näher gezeigten elektrischen Steuereinheit ist. Wenn die Übereinstimmung des Schlüssels 50 mit der Vorrichtung festgestellt ist, schaltet die Steuereinheit ihre elektrischen Ausgänge und/oder Eingänge wirksam. Eine bis dahin bestehende eventuelle Sperre der Fahrzeuglenkung wird entriegelt. Vor allem werden Sensoren 44 wirksam gesetzt, die zu einem hier manuell bedienbaren Betätiger 35 gehören. Mit diesen Sensoren 44 werden die gewünschten verschiedenen Funktionen im Fahrzeug ausgewählt.

Der Betätiger 35 besteht im vorliegenden Fall aus einem Taster, der, wie am besten aus Fig. 2 und 8 zu erkennen ist, in einem Nachbarbereich des gleichen Gehäuses 10 integriert sein kann. Der Taster 35 ist aufgrund einer Axialführung 34 im Sinne des

Druckpfeils 36 von Fig. 8 axial betätigbar und wird mittels einer Rückstellfeder 37 und entsprechende Endanschläge in seine Ausgangsstellung von Fig. 2 zurückgeführt. Welche Betätigungen zu welchen Funktionen im Fahrzeug führen, hängt von der Programmierung der elektrischen Steuereinheit ab. Eine Möglichkeit besteht darin, dass beim ersten Drücken 38 des Tasters 35 ein Radio sowie eine Elektronik im Fahrzeug eingeschaltet wird, z.B. das Parklicht, der Antrieb für Fensterheber, die motorische Sitzverstellung und das Schiebedach. An der Funktionssteuerung der Elektronik können auch noch andere, an sich übliche Steuerglieder im Fahrzeug beteiligt sein, z.B. die Fußbremse. Die vorerwähnte Radioeinstellung erfolgt in diesem Fall ohne Betätigung der Fußbremse. Die weiteren Funktionen im Fahrzeug können auf folgende Weise ausgelöst werden.

Durch ein zweites Drücken 36 des Tasters 35, ohne gleichzeitige Betätigung der Fußbremse, erfolgt beispielsweise die Zündung des Motors. Wird der Taster 35 gedrückt 36 und gleichzeitig die Fußbremse getreten, dann startet der Motor. Wird daraufhin der Taster 35 nochmals gedrückt 36, so geht der Motor wieder aus. Letzteres kann dann mit oder ohne Betätigung der Fußbremse erfolgen.

Diese Funktionen können auch optisch im Bereich des Tasters 35 angezeigt werden, wie am besten anhand von Fig. 8 zu entnehmen ist. Über die Steuerelektronik wird bei der Funktion „Start“ eine erste Diode 46 angesteuert, die ein Teil-Schriftfeld 38 des Tasters 35 gemäß Fig. 4 beleuchtet. Lichttrennwände 39 sorgen für eine entsprechende Teilbelichtung auf der Schauseite des Tasters 35. Bei der Funktion „Stop“ wird durch die Steuereinheit dagegen eine zweite Diode 46' bestromt, worauf dann im Nachbar-Schriftfeld 38' die Beleuchtung eingeschaltet wird und die schauseitige Beschriftung im Taster 35 ablesbar macht.

Die Verriegelung des Schlüssels 50 in der Mittellage 50.2 erfolgt, wie oben beschrieben wurde, durch den Sperrarm 31 der Klinke 30, der über die Schulter 24 auch den Schieber 20 in dessen entsprechende Arbeitsposition 20.2 festhält. Die Klinke 30 befindet sich aufgrund ihrer nicht näher gezeigten Drehfederbelastung und entsprechender Drehanschläge normalerweise in ihrer Sperrposition von Fig. 6. Der Schlüssel 50 ist dabei größtenteils in der Aufnahme 11 versenkt angeordnet und ragt

nur mit einem minimalen Endstück 56 aus der Aufnahme 11 gemäß Fig. 6 heraus. Um den Schlüssel 50 aus der Mittellage 50.2 lösen zu können, muss der Schlüssel 50 zunächst in eine noch tiefere Hublage 50.3 gemäß Fig. 7 im Sinne des dortigen Einsteckpfeils 59 eingedrückt werden. Diese Hublage 50.3 kurz „Endlage“ bezeichnet werden. In Fig. 7 sind die vorausgehenden Hublagen 50.0 bis 50.2 ebenfalls strichpunktiert eingezeichnet.

Zum Übergang von Fig. 6 auf Fig. 7 wird der Schlüssel 50 nur noch um eine verhältnismäßig kleine dritte Hubstrecke 53 gemäß Fig. 7 gegen die axiale Federkraft 41 eingedrückt. Der Schlüssel erreicht dann seine unterste dritte Hublage 50.3, welche natürlich wieder einer entsprechenden Endposition 20.3 des Schiebers 20 entspricht. Diese Endposition 20.3 wird von weiteren Sensoren 47 erfasst, die zu der erfindungsgemäßen Steuereinheit gehören. Im Ansprechfall schaltet die Steuereinheit einen Antrieb 48 ein, der hier aus einem elektrischen Hubmagneten besteht. Dieser Hubmagnet 48 bewegt einen Stößel 49 od. dgl. in eine Arbeitsposition, in welcher er den vorerwähnten Stellarm 32 der Klinke 30 trifft. Weil der Stellarm 32 drehfest mit dem Sperrarm 31 ist, wird durch diese Schwenkbewegung gemäß Fig. 7 der Sperrarm 31 aus seiner bisherigen Sperrposition wegbewegt. Die Schulter 24 wird freigegeben. Die Blockade des Schiebers 20 ist dann aufgehoben. Der Schieber 20 wird aufgrund der wirkenden Federkraft 41 im Sinne des Bewegungspfeils 57 von Fig. 7 automatisch zurückbewegt. Der Sperrarm 31 bleibt dabei solange durch den Hubmagneten 48 in seiner entriegelten Position von Fig. 7, bis die mit dem Schieber 20 mitbewegliche Schulter 24 sich an seinem Sperrende vorbeibewegt hat; d.h. bis kurz nach der aus Fig. 6 erkennbaren Mittellage 50.2 des Schlüssels.

Nach der Entriegelung von Fig. 7 bewegt die axiale Federkraft 41 den Schieber 20, und mit ihm den Schlüssel 50 bis sich wieder die Verhältnisse von Fig. 5 ergeben. Der Schieber 20 stoppt erst in seiner dortigen Ausgangsposition 20.1, wo die Federkraft 41 von dem erwähnten Endanschlag 42 für den Schieber 20 aufgenommen wird. Der Schlüssel 50 steckt aber immer noch in seiner Aufnahme 11. Jetzt ragt der Schlüssel 50 allerdings mit einem größeren Teilstück 28 aus der Aufnahme 11 heraus. Er kann mit der Hand bequem erfasst und manuell ganz im Sinne des Pfeils

57 herausgezogen werden. In der Anfangslage 50.1 von Fig. 5 liegt nämlich wieder die beschriebene kraftschlüssige Halterung des Schlüssels 50 im Schieber 20 vor.

Durch eine plötzliche Rückstellbewegung des Schiebers 20 aus der Endposition von Fig. 2.3 in die Ausgangsposition 20.1 von Fig. 5 könnte der Schlüssel 50 Beschleunigungskräften ausgesetzt sein, die ihn aus der Aufnahme 11 heraus katapultieren, über seine kraftschlüssige Anfangslage 50.1 in Fig. 5 hinaus. Dies lässt sich leicht durch eine geeignete Dämpfungseinrichtung 60 beheben. Diese besteht im vorliegenden Fall aus einem Dämpfungsrad 60, das ortsfest im Gehäuse 10 bei 61 drehgelagert ist, wie aus Fig. 1 und 2 zu erkennen ist. Das Dämpfungsrad 60 steht über ein Stirnrad 62 in Zahneingriff mit einer Zahnstange 63, die mit dem Schieber 20 mitbeweglich ist. Die Zahnstange 63 kann in den vorerwähnten Axialansatz 25 gemäß Fig. 1 und 2 integriert sein, wo auch der Nocken für die Schulter 24 sitzt. Sofern als Sensor 47 ein Mikroschalter verwendet wird, kann der entsprechende Schaltnocken 64 an diesem Ansatz 25 sitzen.

Die erwähnte Steuereinheit ist über die am unteren Gehäuseende vorgesehenen Steckkontakte 65 mit den elektrischen Bauteilen im Inneren des Gehäuses 10 verbunden. Man kann dazu eine auch aus Fig. 8 erkennbare Leiterplatte 66 nutzen, die durch geeignete Zwischenböden 67 in ihrer Position im Inneren des Gehäuses gemäß Fig. 3 gehalten wird.

Wie erwähnt wurde, wird der Schlüssel 50 aus seinem Formschluss in Fig. 6 über Fig. 7 auf elektromechanische Weise freigegeben und selbsttätig in seine Anfangslage 50.1 von Fig. 5 zurückgeführt. Die Bedingung hierfür, welche die erwähnte elektrische Steuereinheit überwacht, ist, dass der Motor des Fahrzeugs ausgeschaltet ist. Wenn man, bei eingeschaltetem Motor, in der Mittellage 50.2 den Schlüssel 50 eindrückt, so wird der beschriebene Hubmagnet 48 nicht wirksam gesetzt; die Klinke 30 bleibt sperrwirksam und fängt den Schlüssel wieder in der Mittellage 50.2 von Fig. 6. Damit ist eine Fehlbedienung der erfindungsgemäßen Vorrichtung ausgeschlossen.



Eine Alternative kann aber darin bestehen, dass bei stehendem Fahrzeug, wo die Räder sich nicht mehr drehen, der Motor noch an ist. Auch dies wird von der elektrischen Steuereinheit registriert. Wird dann wieder im Sinne von Fig. 7 auf den Schlüssel 50 gedrückt, so kann über einen Impulsschalter der Motor ausgeschaltet werden. Der beschriebene Formschluss des Schlüssels 50 wird dann wieder elektromechanisch freigegeben und kann über die Kraftschlussraste aus einer Anfangslage 50.1 in Fig. 5 manuell entnommen werden.

Wie bereits erwähnt wurde, zeigen die Fig. 9 bis 14 den Aufbau und die Wirkungsweise eines zweiten Ausführungsbeispiels der erfindungsgemäßen Vorrichtung, welcher eine eigenständige erfinderische Bedeutung zukommt. Zur Benennung analoger Bauteile sind die gleichen Bezugszeichen wie im ersten Ausführungsbeispiel verwendet, weshalb insoweit die bisherige Beschreibung gilt. Es genügt lediglich auf die Unterschiede einzugehen. Bei dieser Vorrichtung besitzt der Schlüssel 50 die Form einer Scheckkarte.

Die stirnseitige Öffnung 13 der dortigen Aufnahme 11 besteht aus einem Schlitz im Gehäuse 10. Die Abdeckung 14' der Öffnung 13 erfolgt hier durch eine Klappe, deren Aufklapplage in Fig. 10 ausgezogen und deren Zuklapplage bei entnommenem Schlüssel in Fig. 10 strichpunktiert angedeutet ist. Identifikationsmittel für den Schlüssel 50 sind im Gehäuse 10 integriert und bestehen auch in diesem Fall z.B. aus einem Transponder 43. Einen Schieber 20, wie im ersten Ausführungsbeispiel, gibt es nicht. Die Haltemittel und Verriegelungen wirken unmittelbar mit dem Schlüssel 50 zusammen, dessen am besten aus Fig. 11 erkennbarer Scheckkartenumriss 68 in geeigneter Weise profiliert ist. Auch in diesem Fall kann der Schlüssel 50 in der Aufnahme 11 in drei axiale Hublagen 50.1, 50.2 und 50.3 überführt und positioniert werden. Diese drei Hublagen sind in Fig. 9 durch Höhenlinien veranschaulicht und in Fig. 12 bis 14 zusammen mit den damit zusammenwirkenden Bauteile verdeutlicht.

Beim Einschieben 59 des Schlüssels 50 wird zunächst die in Fig. 12 gezeigte Anfangslage 50.1 des Schlüssels 50 erreicht, wo der Schlüssel 50 durch ein Rastgesperre 70 kraftschlüssig im Gehäuse 10 gesichert ist. Auch in diesem Fall besteht das Halteelement 71 aus einer radial federnden Zunge, doch ist diese, im

Gegensatz zum ersten Ausführungsbeispiel, ortsfest im Gehäuseinneren positioniert. Zum Rastgesperre 70 gehört eine Rastvertiefung 55 im Schlüssel 50, die durch ein entsprechendes Kantenprofil seines erwähnten Kantenumrisses 68 erzeugt ist. Ein radialer Vorsprung 75 an der Zunge 71 untergreift kraftschlüssig eine Haltekante 76 an der Rastvertiefung 55.

Weil es in diesem Fall, wie gesagt, einen Schieber nicht gibt, wirken in Fig. 9 angedeutete Rückstellkräfte 41 unmittelbar auf den Schlüssel 50 ein. Maßgeblich dafür sind hier doppelt vorgesehene Rückstellfedern 40, 40', die über einen zugehörigen Stößel 74 bzw. 74', welcher auf die Unterkante 69 des Schlüsselumrisses 68 drücken können. In Fig. 12 ist gerade der eine Stößel 74 in Kantenberührung und übt eine nur geringe Rückstellkraft 41 aus. Die kraftschlüssige Haltekraft der federnden Zunge 41 reicht jedenfalls aus, um die Anfangslage 50.1 des Schlüssels 50 von Fig. 12 sicherzustellen. Eine Entnahme 57 des Schlüssels ist gegen die Wirkung des Rastgesperres 70 in Fig. 12 möglich.

Auch bei diesem zweiten Ausführungsbeispiel lässt sich der Schlüssel 50 von der Anfangslage 50.1 um eine Hubstrecke 52 in die aus Fig. 13 ersichtliche zweite Mittellage 50.2 in der Aufnahme 11 der Vorrichtung weiterschieben 59. Auch in diesem Fall kommt es in der Mittellage 50.2 zu einem Formschluss. Die hierfür maßgeblichen Halteelemente 81 sind in diesem Fall, im Gegensatz zum ersten Ausführungsbeispiel, nicht Bestandteil des Rastgesperres 70, sondern gehören zu einem davon gesonderten Gesperre 80, welches eine mehrfache Funktion zu erfüllen hat. Dieses Gesperre besteht im vorliegenden Fall aus einer Klinke 80, die an einem ortsfesten Lager 84 im Gehäuse 10 schwenkgelagert ist. Eine Klinken-Federbelastung 85 ist bestrebt die Klinke 80 in ihrer aus Fig. 11 ersichtlichen Lage zu halten, wo sie mit einem Stellarm 82 auf den Betätiger 73 eines hier als Mikroschalter ausgebildeten Sensors 72 einwirkt. Dies liegt bereits bei entnommenen Schlüssel gemäß Fig. 11 vor. Dieser Stellarm 82 ist drehfest mit dem vorbeschriebenen Halteelement 81 dieses Verriegelungsgesperres 80 verbunden.

In der in Fig. 12 beschriebenen Ausgangslage 50.1 des eingesteckten Schlüssels 50 kommt das Halteelement 81 der Klinke 80 mit dem Profilbereich 79 der

Umrisskontur 68 in Berührung, durch welche die Klinke 80 gegen ihre Rückschwenkkraft 86 zurückgeschwenkt wird. Dadurch wird der Betätiger 73 des Klinken-Sensors 72 vom Stellarm 82 freigegeben. Das wird von einer auch bei dieser Vorrichtung vorgesehenen elektrischen Steuereinheit festgestellt, an die dieser Klinken-Sensor 72 angeschlossen ist. Der vorerwähnte Transponder 43 wird wirksam gesetzt und stellt fest, ob der „richtige Schlüssel“ eingestellt ist. Nur beim richtigen Schlüssel werden bereits erste Funktionen im Fahrzeug von der Steuereinheit eingeschaltet, z.B. die Spannungsversorgung für ein Radio, für das Parklicht, für einen Antrieb eines Fensterhebers, einer motorischen Sitzverstellung und eines Schiebedachs.

Beim Weiterdrücken 52 des Schlüssels 50 in die bereits erwähnte Mittellage 50.2 von Fig. 13 kommt der Formschluss dadurch zustande, dass das Halteelement 81 ein Hakenende 87 aufweist, welches eine Schulter 88 vom Schlüssel 50 hintergreift. Jetzt ist eine Entnahme des Schlüssels im Sinne des Pfeils 57 blockiert. Bei der Verschiebung 52 des Schlüssels 50 von Fig. 12 auf Fig. 13 ist auch eine Hubarbeit gegen die von der Rückstellfeder 40 bedingte Rückstellkraft 41 ausgeübt worden. In Fig. 13 kommt aber auch die andere Rückstellfeder 40' mit ihrem Stößel 74' an der Unterkante 69 des Schlüsselprofils 68 zur Anlage. Die Schulter 88 gehört zu einem Randausbruch 89 im Scheckkartenumriss 68. Aufgrund seiner Rückschwenkkraft 86 ist daher die Klinke 80 wieder in ihrer bereits in Fig. 11 beschriebenen Ausgangs-Schwenkstellung, wo ihr Stellarm 82 den Betätiger 73 des Klinken-Sensors 72 drückt. In dieser Mittellage 50.2 des Schlüssels schaltet die zugehörige elektrische Steuereinheit die Zündung des Motors im Fahrzeug ein.

In der Mittellage 50.2 von Fig. 13 kommt es auf die kraftschlüssige Haltewirkung des Rastgesperres 70 nicht mehr an. Ein an der federnden Zunge 71 befindlicher radialer Vorsprung 75 greift zwar immer noch in die erwähnte Rastvertiefung 55 des Schlüssels 50 ein, doch liegt dieser Vorsprung 75, im Gegensatz zu Fig. 12, in Abstand von der für den Kraftschluss von Fig. 12 sorgenden Haltekante 76.

Ausgehend von Fig. 13 kann der Schlüssel 50 um eine weitere Hubstrecke 53 in die aus Fig. 14 ersichtliche Endlage 50.3 überführt werden. Dazu ist eine höhere Kraft

erforderlich, weil dem Einschieben 59 nicht nur die bisherige Rückstellfeder 40, sondern auch die zweite Rückstellfeder 40' entgegenwirken. Die Endlage 50.3 wird von einem weiteren Sensor 77 festgestellt. Dieser besteht im vorliegenden Fall ebenfalls aus einem Mikroschalter, dessen Betätiger 78 von der Unterkante 69 des Schlüsselprofils gedrückt wird. Auch dieser Schlüssel-Sensor 77 ist natürlich mit der elektrischen Steuereinheit verbunden. Gleichzeitig stellt die Steuereinheit in Fig. 14 den gedrückten Zustand des Klinken-Sensors 72 fest. Aufgrund ihrer Programmierung schaltet die Steuereinheit den Anlasser des Motors an. Der Motor startet. Dies kann zeitgesteuert erfolgen. Als weitere Bedingung kann die elektrische Steuerung das pedale Betätigen einer Fußbremse überwachen. Auf diese Weise kann ein versehentlicher Start des Motors verhindert werden, wenn die Fußbremse nicht getreten wird. Darüber hinaus wird aber im vorliegenden Fall die Endlage 50.3 des Schlüssels nur impulsweise erreicht, wie aus folgendem Umstand in Fig. 14 zu ersehen ist.

Der vorbeschriebene Halterarm 81 der Klinke 80 kann mit seinem Hakenende 87 sich in dem entsprechend breit bemessenen Randausbruch 89 des Schlüssels von seiner die Verriegelung bedingenden Schulter 88 axial entfernen. Trotz des Eingriffs der Klinke 80 in den Randausbruch 89 erweist sich diese Verriegelung 80 von Fig. 13 als ein „Richtgesperre“, welches zwar das Herausziehen 57 des Schlüssels 50 aus der Mittellage 50.2 von Fig. 13 verhindert, aber ein tieferes Einschieben 59 des Schlüssels in die Endlage 50.3 gestattet. Es handelt sich um eine ähnliche Wirkung, die beim ersten Ausführungsbeispiel von gesonderten Mitteln 30, 31, 24 besorgt werden musste. In diesem zweiten Ausführungsbeispiel übernehmen die Haltemittel 81, 88, 89 der formschlüssigen Verriegelung 80 zugleich die Funktion dieses „Richtgesperres“.

Der vorbeschriebene weitere Abwärtshub 53 des Schlüssels wird auch nicht von den Elementen des kraftschlüssigen Rastgesperres 70 behindert. Wie Fig. 14 zeigt, erlaubt die Größe der Rastausparung 55 eine entsprechend ungestörte Verschiebung des radialen Vorsprungs 75 an der zugehörigen federnden Zunge 71. Der Freiraum bei 89 im Bereich der Klinke 80 einerseits und bei 55 im Bereich des Rastgesperres 70 andererseits erlauben es, dass die von den Rückstellfedern 40, 40' ausgeübte

Rückstellkraft 41 den Schlüssel 50 aus Fig. 14 wieder in die Mittellage 50.2 von Fig. 13 zurückführt. Die Mittellage 50.2 ist ja durch das wie ein „Sperrarm“ wirkende Halteelement 81 der Klinke 80 gesichert; das Hakenende 87 hintergreift wieder die Schulter 88 vom Schlüssel 50. Es liegt dann wieder die im Zusammenhang mit Fig. 13 bereits beschriebene Stellung „Zündung“ des Motors vor. Der vorausgehend in Fig. 14 gestartete Motor läuft in Fig. 13 weiter.

Um den Motor auszuschalten, braucht, ausgehend von der Mittellage 15.2 des Schlüssels 50 in Fig. 13 der Schlüssel 50 nur noch erneut, ein zweites Mal, in seine Endlage von Fig. 14 gedrückt zu werden. Es kommt dabei nicht darauf an, ob die Fußbremse dabei ebenfalls getreten oder nicht getreten wird. Stattdessen kann die elektrische Steuerung über einen Sensor den Bremskontakt oder die Raddrehung vom Fahrzeug sensieren. Die elektrische Steuereinheit schaltet aber auch einen auf die Klinke 80 wirkenden Antrieb 48 gemäß Fig. 9 ein. Dieser besteht auch in diesem zweiten Ausführungsbeispiel aus einem Hubmagneten 48, der über einen Stößel 49 auf einen drehfest mit der Klinke 80 verbundenen Lösearm 83 einwirkt. Die Klinke 80 wird in die strichpunktiert in Fig. 9 verdeutlichte Entriegelungsstellung 80' überführt. Dann ist die Schulter 88 frei. Weil die Rückstellfeder 40 eine Rückstellkraft 41 ausübt, schiebt sie den Schlüssel 50 aus der Mittellage 50.2 von Fig. 13 bzw. 9 wieder in die Anfangslage 50.1 von Fig. 12 zurück. Dann ist der Formschluss beseitigt. Das Verriegelungsgesperre 80 ist gemäß Fig. 12 durch den beschriebenen Profildbereich 79 entriegelt. Es liegt wieder nur der Kraftschluss des Rastgesperres 70 vor. Die manuelle Entnahme 57 des Schlüssels 50 ist in Fig. 12 wieder ohne weiteres möglich. Beim Klinken-Sensor 72 befindet sich der Betätiger 73 wieder im umgedrückten Zustand.

Ausgehend von der Anfangslage 50.1 des Schlüssels 50 in Fig. 12 kann der Schlüssel 50 natürlich alternativ, durch erneutes zweistufiges Drücken 59, über die Mittellage 50.2 von Fig. 13, wo sich die Zündung von der Steuereinheit wieder einschaltet, die Endlage 50.3 gemäß Fig. 14 gebracht werden, wo der Motor gestartet wird. Eine Fehlbedienung ist ausgeschlossen.

Auch in diesem zweiten Ausführungsbeispiel kann der mit der Klinke 80 zusammenwirkende Hubmagnet 48 dazu genutzt werden, um einen „falschen Schlüssel“ aus der Vorrichtung zu entfernen. Es könnten zunächst die Haltelage 50.1 von Fig. 12 und möglicherweise auch die Endlage 50.2 von Fig. 13 mit einem falschen Schlüssel erreicht sein. Spätestens dann identifiziert aber der Transponder 43 od. dgl. den „falschen Schlüssel“. Daraufhin schaltet die elektrische Steuereinheit den Hubmagneten 48 ein, der über seinen Stößel 49 die Klinke 80 in ihre beschriebene Entriegelungsstellung 80' überführt. Die von den Rückstellfedern 40 ausgeübte Rückstellkraft 41 drückt dann den falschen Schlüssel in die Anfangslage 50.1 von Fig. 12 zurück. Der Motor konnte mit dem falschen Schlüssel nicht gestartet werden.

Sofern das Fahrzeug mit einem „Automatikgetriebe“ versehen ist, muss bei der Schlüsselentnahme 57 in der Anfangsstellung 50.1 von Fig. 12 der Wählhebel auf den Stellungen „B“ oder „N“ stehen. Außerdem ist bei dieser Vorrichtung ebenso wie beim ersten Ausführungsbeispiel eine elektrische Lenkradverriegelung vorgesehen, die bei entnommenen Schlüssel für eine Verriegelung des Lenkrads sorgt. Befindet sich der richtige Schlüssel in der Aufnahme 11, der dann vom Transponder 43 festgestellt wird, so wird die Lenkradverriegelung unwirksam gesetzt. Außerdem ist ein nicht näher gezeigter Sensor im Bereich der Aufnahme 11 vorgesehen, welcher in beiden Ausführungsbeispielen eine Verriegelung des Lenkrads dann ausschließt, solange der Schlüssel 50 sich in einen seiner drei Hublagen 50.1, 50.2 oder 50.3 befindet. Erst wenn der Schlüssel 57 aus dem Gehäuse 10 ganz entnommen ist, wird die Lenkradverriegelung wirksam gesetzt. Ebenso wird in allen Fahrtstellungen eines Automatik-Getriebes eine Auswurfbewegung auf den in der Mittellage 50.2 befindlichen Schlüssel 50 der Schlüssel nicht freigegeben und die Lenkradsicherung nicht in ihre Verriegelungsposition überführt. So lassen sich leicht Fehlbedienungen verhindern.

Im Gehäuse kann eine aus Fig. 9 und 10 ersichtliche Beleuchtung 90 vorgesehen sein, die beim Öffnen der Tür für eine bestimmte Zeit aktiviert wird. Dann wird der Einführschlitz 13 beleuchtet und erleichtert das Einführen der Karte 50.

## B e z u g s z e i c h e n l i s t e :

- 10 Gehäuse
- 11 Aufnahme
- 12 Kontur der Armatur
- 13 stirnseitige Öffnung von 11
- 14 Abdeckung von 11
- 14' Abdeckklappe (Fig. 10)
- 14.1 Ausschubstellung von 14 (Fig. 1, 2)
- 14.2 Einschubstellung von 14 (Fig. 6 bis 7)
- 15 Abdeck-Druckfeder für 14
- 16 radiale Aussparung von 10 für 23
- 17 Blende für 13
- 18 axiales Führungsmittel bei 17, Steg
- 19 radiale Stützfläche für 23 von 10
- 20 Schieber
- 20.1 erste Axialposition von 20, Ausgangsposition (Fig. 1 bis 5)
- 20.2 zweite Axialposition von 20, Arbeitsposition (Fig. 6)
- 20.3 dritte Axialposition von 20, Endposition (Fig. 7)
- 21 Halteelement für 50, federnde Zunge
- 22 erster Endanschlag für 14, Halteelement für 50, federnder Vorsprung
- 23 Gegenvorsprung an 21
- 24 Schulter für 31, Nocken (Richtgesperre)
- 25 Axialansatz von 20
- 26 Innenbund in 25 für 40
- 27 Punktlinie, Verschiebungsweg von 24
- 28 herausragendes Teilstück von 50 (Fig. 5)
- 29 zweiter Endanschlag von 14 (Fig. 5)
- 30 Riegel, Klinke (Richtgesperre)
- 31 Sperrarm von 30 (Richtgesperre)

- 32 Lösearm von 30
- 33 Schwenklager von 30
- 34 Axialführung für 35 (Fig. 8)
- 35 Betätiger, Taster
- 36 Druckbetätigungspfeil zur Tasterbetätigung für 35 (Fig. 8)
- 37 Rückstellfeder für 35
- 38 Schriftfeld-Teil von 35 für 46
- 38' Schriftfeld-Rest von 35 für 46'
- 39 Lichttrennwand an 35 (Fig. 8)
- 40 Rückstellfeder für 20 (Fig. 1 bis 8) bzw. für 50 (Fig. 9 bis 14)
- 40' weitere Rückstellfeder für 50 (Fig. 9 bis 14)
- 41 Pfeil der axialen Rückstellkraft von 20 bzw. 50, axiale Federbelastung
- 42 Endanschlag an 10 für 20 (Fig. 5)
- 43 Transponder der elektronischen Steuereinheit
- 44 Sensor für 35 (Fig. 2, 8)
- 45 Gehäusehülse für 25
- 46 Diode für „Start“ in 35 (Fig. 8)
- 46' Diode für „Stop“ in 35 (Fig. 8)
- 47 Sensor für 50.3
- 48 Antrieb, Hubmagnet
- 49 Stößel von 48
- 50 elektronischer Schlüssel
- 50.0 Berührungslage von 50 (Fig. 1, 2)
- 50.1 erste axiale Hublage von 50, Anfangslage (Fig. 5)
- 50.2 zweite axiale Hublage von 50, Mittellage (Fig. 6)
- 50.3 dritte axiale Hublage von 50, Endlage (Fig. 7)
- 51 erste Hubstrecke von 50 (Fig. 5)
- 52 zweite Hubstrecke von 50 (Fig. 6)
- 53 dritte Hubstrecke von 50 (Fig. 7)
- 54 axiales Führungsmittel an 50, Längsnut
- 55 Halteelement, Rastvertiefung
- 56 herausragendes Endstück von 50 bei 50.2 (Fig. 6)
- 57 Pfeil des Rückschubs, Herausziehbewegung von 50 aus 11



- 58 Vorderstück von 50
- 59 Pfeil der Einschubbewegung von 50 in 11
- 60 Dämpfungseinrichtung für 20, Dämpfungsrad
- 61 Drehachse von 60
- 62 Stirnrad von 60
- 63 Zahnstange für 62
- 64 Schaltnocken für 47 (Fig. 2)
- 65 Steckkontakt an 10
- 66 Leiterplatte
- 67 Zwischenboden (Fig. 3)
- 68 Kartenumriss von 50 (Fig. 11), Schlüsselprofil
- 69 Unterkante von 50
- 70 kraftschlüssiges Rastgesperre
- 71 Halteelement von 70, federnde Zunge
- 72 Klinken-Sensor
- 73 Betätiger von 72
- 74 Stößel für 40
- 74' Stößel für 40'
- 75 federnder Vorsprung an 71
- 76 Haltekante von 55 für 50 (Fig. 12)
- 77 Schlüssel-Sensor
- 78 Betätiger von 77
- 79 Profilbereich von 68 für Abstützung von 81
- 80 Richtgesperre, Klinke (Verriegelungsstellung)
- 80' Entriegelungsstellung von 80
- 81 Halteelement von 80, Sperrarm
- 82 Stellarm von 80
- 83 Lösearm von 80
- 84 Schwenklager für 80
- 85 Klinken-Federbelastung
- 86 Rückschwenk-Kraft von 85 auf 80
- 87 Hakenende von 81
- 88 Schulter für 87 von 80

- 89 Randausbruch von 68 für 87
- 90 Beleuchtung in 11 (Fig. 10)

## P a t e n t a n s p r ü c h e :

- 1.) Vorrichtung zum Starten eines Fahrzeug-Motors mittels eines elektronischen Schlüssels (50), der gegebenenfalls ein Scheckkarten-Format aufweist,

mit einer zum Einstecken (59) des Schlüssels (50) dienenden Aufnahme (11) im Fahrzeug,

wobei der in der Aufnahme (11) eingesteckte Schlüssel (50) manuell in verschiedene Schlüssellagen überführbar ist

und die Schlüssellagen von Sensoren einer elektronischen Steuereinheit überwacht und zur Steuerung von verschiedenen Funktionen des Motors und gegebenenfalls weiterer Zusatzgeräte im Kraftfahrzeug, wie einem Radio, genutzt werden,

d a d u r c h g e k e n n z e i c h n e t ,

dass der eingesteckte Schlüssel (50) in der Aufnahme (11) unverdrehbar und mindestens zwischen drei zueinander axial versetzten Hublagen (50.1, 50.2, 50.3) längsverschiebbar (51, 52, 53) ist, nämlich,

beim anfänglichen Einstecken (59), zunächst in eine den Schlüssel (50) im vorderen Bereich der Aufnahme (11) nur kraftschlüssig sichernden Anfangslage (50.1),

dann, beim Weiterschieben (59) um eine erste Hubstrecke (52), in eine den Schlüssel (50) im mittleren Bereich der Aufnahme (11) formschlüssig sichernden Mittellage (50.2),

welche zwar ein manuelles Herausziehen (57) des Schlüssels (50) aus der Aufnahme (11) verhindert, aber ein Weiterschieben (59) des Schlüssels (50) erlaubt,

und schließlich beim Weiterschieben (59) um eine zweite Hubstrecke (53) in eine den Schlüssel (50) im hinteren Bereich der Aufnahme (11) positionierende Endlage (50.3),

dass der Schlüssel (50) mindestens in seiner Mittel- und Endlage (50.2, 50.3) in Richtung seiner Anfangslage (50.1) entweder unmittelbar oder mittelbar (20) von einer Rückstellfeder (40) axial federbelastet (41) ist, wobei die Sensoren der Steuereinheit mindestens einige der drei Schlüssel-Hublagen (50.1, 50.2, 50.3) überwachen.

- 2.) Vorrichtung nach Anspruch 1, dadurch gekennzeichnet, dass wenigstens ein manueller und/oder pedaler Betätiger (35) im Fahrzeug angeordnet ist und mit der Steuereinheit in Wirkverbindung steht

und dass eine Betätigung des Betätigers (35) die Auswahl der verschiedenen Funktionen des Fahrzeugs mitbestimmt.

- 3.) Vorrichtung nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass der Schlüssel (50) beim Weiterschieben (59) aus der Mittellage (50.2) seine Endlage (50.3) nur impulsweise erreicht

und dass - nach Beendigung des manuellen Einschubdrucks - die Rückstellfeder (40) den Schlüssel (50) selbsttätig wieder in die Mittellage (50.2) oder die Anfangslage (50.1) zurückschiebt (75).

- 4.) Vorrichtung nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass die Aufnahme (11) sowohl ein den Kraftschluss erzeugendes Rastgesperre (21, 22, 55; 70) für den eingesteckten Schlüssel (50) als auch ein mittelbar (20) oder unmittelbar mit dem Schlüssel (50) zusammenwirkendes Richtgesperre (24, 30, 31; 80) besitzt,

dass das Rastgesperre (21, 22, 55; 70) mindestens in der Anfangslage (50.1), aber das Richtgesperre (24, 30, 31; 80) sowohl in der Mittellage (50.2) als auch in der Endlage (50.3) des Schlüssels (50) wirksam sind

und dass bei wirksamem Richtgesperre (24, 30, 31; 80) das Weiterschieben (59) des Schlüssels (50) aus der Mittellage (50.2) in die Endlage (50.3) und das rückstellfederbedingte Zurückschieben (57) des Schlüssels (50) aus der Endlage (50.3) in die Mittellage (50.2) zwar möglich sind,

aber ein Zurückschieben (57) des Schlüssels (50) aus der Mittellage (50.2) in die Anfangslage (50.1) verhindert ist.

- 5.) Vorrichtung nach Anspruch 4, dadurch gekennzeichnet, dass beim Einschieben (59) des Schlüssels (50) in die Anfangslage (50.1) das Rastgesperre (21, 22, 50; 70) und beim Einschieben (59) in die Mittellage (50.2) das Richtgesperre (24, 30, 31; 80) selbsttätig wirksam setzbar sind

und dass die Steuereinheit auf ein einmaliges oder mehrmaliges Eindrücken (59) des Schlüssels (50) zwischen der Mittellage (50.2) in die Endlage (50.3) anspricht und das Richtgesperre (24, 30, 31; 80) solange unwirksam setzt, bis die Rückstellfeder-Kraft (41) den Schlüssel (50) in die Anfangslage (50.1) zurückgeschoben (57) hat.

- 6.) Vorrichtung nach Anspruch 5, dadurch gekennzeichnet,

dass das Richtgesperre einen seinerseits federbelasteten (85) Riegel (30; 80) aufweist, der in den axialen Weg (27) einer entweder unmittelbar oder mittelbar (20) mit dem Schlüssel (50) mitverschieblichen Schulter (24; 88) hineinragt und die Schulter (24; 88) in der Endlage (50.3) des Schlüssels (50) hintergreift

und dass die Steuereinheit im Ansteuerungsfall den Riegel (30; 80) gegen seine Riegel-Federbelastung (86) aus dem axialen Weg der Schulter (24; 88) herausbewegt.

- 7.) Vorrichtung nach Anspruch 6, dadurch gekennzeichnet, dass der Riegel aus einer federbelasteten Klinke (30; 80) besteht, wobei die Klinke (30; 80) außer einem mit der Schulter (21; 88) zusammenwirkenden Sperrarm (31; 81) einen damit drehfesten Lösearm (32) besitzt,

und dass der Lösearm (32; 83) mit einem Antrieb (48), wie einem elektrischen Hubmagneten (48), verbunden ist, der von der elektrischen Steuereinheit gesteuert wird.

- 8.) Vorrichtung nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass in der Aufnahme (11) elektronische Identifikationsmittel für den Schlüssel (50) angeordnet sind, die mit der elektrischen Steuereinheit in Wirkverbindung stehen,

und dass bei Ermittlung eines falschen Schlüssels (50) der Antrieb (48) für die Klinke (30; 80) wirksamgesetzt wird und den Riegel freigibt,

wodurch der falsche Schlüssel (50) von der Rückstellfederkraft (41) in seine Anfangslage (50.1) in der Aufnahme (11) zurückgeschoben wird.

- 9.) Vorrichtung nach Anspruch 8, dadurch gekennzeichnet, dass die elektronischen Identifikationsmittel aus einem Transponder (48) bestehen.
- 10.) Vorrichtung nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, dass die kraftschlüssigen Halteelemente (21; 81) des Rastgesperres einerseits aus einem federnden Glied (22) im Bereich der Aufnahme (11) und andererseits aus einer Rastvertiefung (59) am Schlüssel (50) bestehen.
- 11.) Vorrichtung nach einem der Ansprüche 1 bis 10, dadurch gekennzeichnet, dass der Schlüssel (50) die Umrissform (68) einer Scheckkarte hat.
- 12.) Vorrichtung nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, dass das Rastgesperre (70) und Richtgesperre (80) ortsfest in einem die Aufnahme (11) umschließenden Gehäuse (10) angeordnet sind,
- dass nicht nur die Rastvertiefung (55) für das Rastgesperre (70), sondern auch die Schulter (88) des Richtgesperres (80) unmittelbar am Umrissprofil (68) des Schlüssels (50) sich befinden
- und dass die Verriegelungs-Elemente (81) des Richtgesperres (80) zugleich die formschlüssigen Halteelemente für den Schlüssel (59) sind.
- 13.) Vorrichtung nach einem der Ansprüche 6 bis 12, dadurch gekennzeichnet, dass die Klinke (80) des Richtgesperres einen drehfest mit dem Sperr- und Lösearm (81, 83) ausgebildeten Stellarm (82) aufweist
- und der Stellarm (82) auf einen Klinken-Sensor (72) einwirkt.

- 14.) Vorrichtung nach Anspruch 13, dadurch gekennzeichnet, dass die Sperrstellung der Klinke (80) durch die Klinken-Federbelastung (85) und gegebenenfalls einen Drehanschlag bestimmt ist,

dass die Sperrstellung sowohl bei herausgezogenem Schlüssel (50), also bei leerer Aufnahme (11), als auch bei einem in der Mittellage (50.2) und in der Endlage (50.3) befindlichen Schlüssel (50) vorliegt

und dass der Klinken-Sensor (72) vom Stellarm (82) zwar in der Sperrstellung der Klinke (80) betätigt wird,

aber in der Anfangslage (50.1) des Schlüssels (50) die Klinke (80) von einem Profilabschnitt (79) des Schlüssel-Umrissprofils (68) aus ihrer Sperrstellung gegen die Klinken-Federbelastung (86) verschwenkt (80') ist und den Klinken-Sensor (72) freigibt.

- 15.) Vorrichtung nach Anspruch 14, dadurch gekennzeichnet, dass die Aufnahme (11) außer dem Klinken-Sensor (72) einen ebenfalls mit der Steuereinheit in Verbindung stehenden Schlüssel-Sensor (77) besitzt, der die Endlage (50.3) des Schlüssels (50) überwacht.

- 16.) Vorrichtung nach einem der Ansprüche 1 bis 15, dadurch gekennzeichnet, dass die auf den Schlüssel (50) wirkende axiale Rückstellkraft (41) sich in Abhängigkeit von dessen Hublage (50.1, 50.2, 50.3) in der Aufnahme (11) stufenartig verändert

und dass die Rückstellkraft (41) in der Anfangslage (50.1) des Schlüssels (50) geringer als in der Mittellage (50.2) und der Endlage (50.3) ist.



17.) Vorrichtung nach einem der Ansprüche 1 bis 16, dadurch gekennzeichnet, dass der zur Auswahl verschiedener Funktionen im Fahrzeug dienende manuelle oder pedale Betätiger (35) zwar in der Mittellage (50.2) des Schlüssels wirksam, aber in allen übrigen Lagen (50.0, 50.1, 50.3) des Schlüssels (50) unwirksam ist.

18.) Vorrichtung nach einem der Ansprüche 1 bis 11 und 17 mit einer Aufnahme (11), deren Öffnung (13) normalerweise von einer federnden (15) Abdeckung (14) verschlossen (14.1) ist,

wobei die Abdeckung (14) beim Einstecken (59) vom Schlüssel (50) gegen die Abdeck-Federbelastung (15) weggedrückt (14.2) wird,

d a d u r c h g e k e n n z e i c h n e t ,

dass die Abdeckung (14) Bestandteil eines im Gehäuse (10) der Aufnahme (11) axial beweglichen Schiebers (20) ist,

dass der Schieber (20) beim Einstecken (59) das Vorderstück (48) des Schlüssels (50) aufnimmt und der Schieber (20) sowohl die kraftschlüssig als auch formschlüssig auf den Schlüssel (50) einwirkenden Haltemittel (21, 22, 55) besitzt, wobei diese Haltemittel den Schlüssel (50) im Schieber (20) sichern,

dass der Schieber (20) durch die Axialbewegung (59) des Schlüssels (50) in verschiedene Axialpositionen (20.1, 20.2, 20.3) überführbar ist, welche die verschiedenen Hublagen (50.1, 50.2, 50.3) des Schlüssels (50) bestimmen,

und dass der Schieber (20) axial federbelastet (40) ist und dadurch auf den eingesteckten Schlüssel (50) ausgeübte Rückstellkraft (41) erzeugt,

und dass der Schieber (20) in seiner die Mittellage (50.2) des Schlüssels (50) bestimmenden mittleren Axialposition (50.2) von einem federnden Riegel (30) eines Richtgesperres festgehalten wird und dieses Richtgesperre mittelbar, über den Schieber (20), auf den Schlüssel (50) wirkt.

- 19.) Vorrichtung nach Anspruch 18, dadurch gekennzeichnet, dass der Schieber (20) sowohl in der Anfangslage (50.1) des eingesteckten Schlüssels (50) als auch bei herausgezogenem Schlüssel sich in der gleichen Ausgangsposition (20.1) im Gehäuse (10) der Aufnahme (11) befindet,

und dass die Ausgangsposition (50.1) durch die auf den Schieber (20) wirkende axiale Federkraft (41) einerseits und einen Endanschlag (42) im Gehäuse (10) der Aufnahme (11) andererseits bestimmt ist.

- 20.) Vorrichtung nach Anspruch 19, dadurch gekennzeichnet, dass die Abdeckung (14) für die Öffnung (13) der Aufnahme (11) ihrerseits zwischen zwei Stellungen (14.1, 14.2) im Schieber (20) axial verschieblich ist,

dass diese beiden Stellungen (14.1, 14.2) durch einen vorderen und einen hinteren Endanschlag (22, 29) im Schieber (20) bestimmt sind,

dass die Abdeck-Federbelastung (15) bestrebt ist, die Abdeckung (14) axial gegen den vorderen Endanschlag (22) zu drücken,

und dass der vordere Endanschlag (22) und die Abdeck-Federbelastung (15) die bei herausgezogenem Schlüssel (50) sich ergebende abdeckwirksame Ausschubstellung (14.1) der Abdeckung (14) an der Öffnung (13) bestimmen.

- 21.) Vorrichtung nach Anspruch 20, dadurch gekennzeichnet, dass bei eingestecktem Schlüssel (50) die Abdeckung (14) sich in einer durch den

hinteren Endanschlag (29) am Schieber (20) bestimmten Einschubstellung (14.2) befindet

und dass diese Einschubstellung (14.2) der Abdeckung (14) in allen drei axialen Hublagen des Schlüssels (50) vorliegt.

22.) Vorrichtung nach einem der Ansprüche 18 bis 21, dadurch gekennzeichnet, dass die gleichen Halteelemente (21, 22, 55), welche die kraftschlüssige Verbindung zwischen dem Schlüssel (50) und dem Schieber (20) erzeugen, auch bei der formschlüssige Verbindung zwischen dem Schlüssel (50) und dem Schieber (20) beteiligt sind.

23.) Vorrichtung nach Anspruch 22, dadurch gekennzeichnet, dass die am Schieber (20) befindlichen kraftschlüssigen Halteelemente (21, 22) einen federnden Vorsprung (22) aufweisen

dass dem Vorsprung (22) ein Gegenvorsprung (23) auf seiner dem Gehäuse (10) der Aufnahme (11) zugekehrten Rückseite zugeordnet ist,

dass dieser Gegenvorsprung (23) in der die Haltelage (50.1) des Schlüssels (50) kennzeichnenden Ausgangsposition (20.1) des Schiebers (20) mit einer Aussparung (16) im Gehäuse (10) radial ausgerichtet ist, in welchen der Gegenvorsprung (23) federnd ausweicht, wenn der Schlüssel (50) eingesteckt (59) wird,

und dass dem Gegenvorsprung (23) eine radiale Stützfläche (19) im Gehäuse (10) zugeordnet ist, die das federnde Glied (22) radial versteift, wenn der Schieber (20) vom Schlüssel (50) aus seiner Ausgangsposition (20.1) in eine der tiefer gelegenen Axialpositionen (20.2, 20.3) weiterbewegt wird.

- 24.) Vorrichtung nach einem der Ansprüche 17 bis 23, dadurch gekennzeichnet, dass der axialbewegliche Schieber (20) ein mit einer Dämpfungseinrichtung (60) versehen ist,

und dass die Dämpfungseinrichtung (60) die federbedingte (40) axiale Rückbewegung (57) des im Schieber (20) aufgenommenen Schlüssels (50) aus dessen Endlage (50.3), über die Mittellage (50.2), bis zur Anfangslage (50.1) bremst.

- 25.) Vorrichtung nach einem der Ansprüche 1 bis 24, dadurch gekennzeichnet, dass die zur Unterscheidung der ausgewählten Funktion dienende Steuereinheit auch auf Betätigung bzw. Nichtbetätigung weiterer Steuerglieder im Fahrzeug anspricht, wie eine Fußbremse.

- 26.) Vorrichtung nach einem der Ansprüche 1 bis 24, dadurch gekennzeichnet, dass die zur Unterscheidung der ausgewählten Funktionen dienende Steuereinheit auf eine Nicht-Betätigung weiterer Steuerglieder im Fahrzeug anspricht.

- 27.) Vorrichtung nach einem der Ansprüche 1 bis 26, dadurch gekennzeichnet, dass der für die verschiedenen Funktionen im Kraftfahrzeug dienende Betätiger einen Taster (35) umfasst

und dass die elektrische Steuereinheit die Anzahl und/oder die Reihenfolge der verschiedenen Betätigungen (36) unterscheidet und dementsprechend die ausgewählten Funktionen im Kraftfahrzeug auslöst.

28.) Vorrichtung nach einem der Ansprüche i bis 27, dadurch gekennzeichnet, dass zum unverdrehbaren Einstecken axiale Führungsmittel (18, 54) zwischen dem Schlüssel (50) einerseits und der Aufnahme (11) andererseits vorgesehen sind.

29.) Vorrichtung nach Anspruch 28, dadurch gekennzeichnet, dass die zur Aufnahme (11) gehörenden axialen Führungsmittel (18) in einer die Öffnung (13) der Aufnahme umschließenden Blende (17) angeordnet sind

und dass im Bereich der am Schlüssel (50) vorgesehenen Führungsmittel (54) auch die Angriffsstellen (55) für die kraftschlüssig und/oder formschlüssig wirksamen Halteelemente (21, 22, 23) des Rast- und/oder Richtgesperres angeordnet sind.

**GEÄNDERTE ANSPRÜCHE**

{beim Internationalen Büro am 09. Januar 2001 (09.01.01) eingegangen;  
ursprüngliche Ansprüche 1-29 durch neue Ansprüche 1-20 ersetzt (8 Seiten)}

- 1.) Vorrichtung zum Starten eines Fahrzeug-Motors mittels eines elektronischen Schlüssels (50), der gegebenenfalls ein Scheckkarten-Format aufweist.

mit einer zum Einstecken (59) des Schlüssels (50) dienenden Aufnahme (11) im Fahrzeug,

wobei der in der Aufnahme (11) eingesteckte Schlüssel (50) unverdrehbar und mindestens zwischen drei zueinander axial versetzten Hublagen (50.1, 50.2, 50.3) längsverschiebbar (51, 52, 53) ist

wobei der Schlüssel (50) in seiner Endlage (50.3) in Richtung seiner Anfangslage (50.1) entweder unmittelbar oder mittelbar von einer Rückstellfeder (40) axial federbelastet (41) ist und

einige der drei Schlüssel-Hublagen (50.1, 50.2, 50.3) von Sensoren einer Steuereinheit überwacht und zur Steuerung von verschiedenen Funktionen des Motors genutzt werden,

d a d u r c h g e k e n n z e i c h n e t ,

dass der Schlüssel (50) auch in seiner Mittellage (50.2) in Richtung seiner Anfangslage (50.1) von einer Rückstellfeder (40) axial federbelastet (41) ist und

beim Einschieben (59) des Schlüssels (50) in die Anfangslage (50.1) ein Rastgesperre (21, 22; 50; 70) und beim Einschieben (59) in die Mittellage (50.2) ein mit dem Schlüssel (50) mittelbar (20) oder unmittelbar zusammenwirkendes Richtgesperre (24; 30, 31; 80) selbsttätig wirksam setzbar sind und

dass die Steuereinheit auf ein einmaliges oder mehrmaliges Eindrücken (59) des Schlüssels (50) zwischen der Mittellage (50.2) in die Endlage (50.3) anspricht und das Richtgesperre (24; 30, 31; 80) solange unwirksam setzt, bis die Rückstellfederkraft (41) den Schlüssel (50) selbsttätig in die Anfangslage (50.1) zurückgeschoben (57) hat.

- 2.) Vorrichtung nach Anspruch 1, dadurch gekennzeichnet,

dass das Richtgesperre einen seinerseits federbelasteten (85) Riegel (30; 80) aufweist, der in den axialen Weg (27) einer entweder unmittelbar oder mittelbar (20) mit dem Schlüssel (50) mitverschieblichen Schulter (24; 88) hineinragt und die Schulter (24; 88) in der Endlage (50.3) des Schlüssels (50) hintergreift

und dass die Steuereinheit im Ansteuerungsfall den Riegel (30; 80) gegen seine Riegel-Federbelastung (86) aus dem axialen Weg der Schulter (24; 88) herausbewegt.

- 3.) Vorrichtung nach Anspruch 2, dadurch gekennzeichnet, dass der Riegel aus einer federbelasteten Klinke (30; 80) besteht, wobei die Klinke (30; 80) außer einem mit der Schulter (21; 88) zusammenwirkenden Sperrarm (31; 81) einen damit drehfesten Lösearm (32) besitzt,

und dass der Lösearm (32; 83) mit einem Antrieb (48), wie einem elektrischen Hubmagneten (48), verbunden ist, der von der elektrischen Steuereinheit gesteuert wird.

- 4.) Vorrichtung nach einem der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass in der Aufnahme (11) elektronische Identifikationsmittel für den Schlüssel

(50) angeordnet sind, die mit der elektrischen Steuereinheit in Wirkverbindung stehen,

und dass bei Ermittlung eines falschen Schlüssels (50) der Antrieb (48) für die Klinke (30; 80) wirksamgesetzt wird und den Riegel freigibt,

wodurch der falsche Schlüssel (50) von der Rückstellfederkraft (41) in seine Anfangslage (50.1) in der Aufnahme (11) zurückgeschoben wird.

5.) Vorrichtung nach Anspruch 4, dadurch gekennzeichnet, dass die elektronischen Identifikationsmittel aus einem Transponder (43) bestehen.

6.) Vorrichtung nach einem der Ansprüche 2 bis 5, dadurch gekennzeichnet, dass die Klinke (80) des Richtgesperres einen drehfest mit dem Sperr- und Lösearm (81, 83) ausgebildeten Stellarm (82) aufweist

und der Stellarm (82) auf einen Klinken-Sensor (72) einwirkt.

7.) Vorrichtung nach Anspruch 6, dadurch gekennzeichnet, dass die Sperrstellung der Klinke (80) durch die Klinken-Federbelastung (85) und gegebenenfalls einen Drehanschlag bestimmt ist,

dass die Sperrstellung sowohl bei herausgezogenem Schlüssel (50), also bei leerer Aufnahme (11), als auch bei einem in der Mittellage (50.2) und in der Endlage (50.3) befindlichen Schlüssel (50) vorliegt

und dass der Klinken-Sensor (72) vom Stellarm (82) zwar in der Sperrstellung der Klinke (80) betätigt wird,



aber in der Anfangslage (50.1) des Schlüssels (50) die Klinke (80) von einem Profilabschnitt (79) des Schlüssel-Umrissprofils (68) aus ihrer Sperrstellung gegen die Klinken-Federbelastung (86) verschwenkt (80') ist und den Klinken-Sensor (72) freigibt.

- 8.) Vorrichtung nach Anspruch 7, dadurch gekennzeichnet, dass die Aufnahme (11) außer dem Klinken-Sensor (72) einen ebenfalls mit der Steuereinheit in Verbindung stehenden Schlüssel-Sensor (77) besitzt, der die Endlage (50.3) des Schlüssels (50) überwacht.
  
- 9.) Vorrichtung nach einem der Ansprüche 1 bis 8, dadurch gekennzeichnet, dass die auf den Schlüssel (50) wirkende axiale Rückstellkraft (41) sich in Abhängigkeit von dessen Hublage (50.1, 50.2, 50.3) in der Aufnahme (11) stufenartig verändert  
  
und dass die Rückstellkraft (41) in der Anfangslage (50.1) des Schlüssels (50) geringer als in der Mittellage (50.2) und der Endlage (50.3) ist.
  
- 10.) Vorrichtung nach einem der Ansprüche 1 bis 9, dadurch gekennzeichnet, dass der zur Auswahl verschiedener Funktionen im Fahrzeug dienende manuelle oder pedale Betätiger (35) zwar in der Mittellage (50.2) des Schlüssels wirksam, aber in allen übrigen Lagen (50.0, 50.1, 50.3) des Schlüssels (50) unwirksam ist.
  
- 11.) Vorrichtung nach einem der Ansprüche 1 bis 5 und 10 mit einer Aufnahme (11), deren Öffnung (13) normalerweise von einer federnden (15) Abdeckung (14) verschlossen (14.1) ist,

wobei die Abdeckung (14) beim Einstecken (59) vom Schlüssel (50) gegen die Abdeck-Federbelastung (15) weggedrückt (14.2) wird,

d a d u r c h g e k e n n z e i c h n e t ,

dass die Abdeckung (14) Bestandteil eines im Gehäuse (10) der Aufnahme (11) axial beweglichen Schiebers (20) ist,

dass der Schieber (20) beim Einstecken (59) das Vorderstück (48) des Schlüssels (50) aufnimmt und der Schieber (20) sowohl die kraftschlüssig als auch formschlüssig auf den Schlüssel (50) einwirkenden Haltemittel (21, 22, 55) besitzt, wobei diese Haltemittel den Schlüssel (50) im Schieber (20) sichern,

dass der Schieber (20) durch die Axialbewegung (59) des Schlüssels (50) in verschiedene Axialpositionen (20.1, 20.2, 20.3) überführbar ist, welche die verschiedenen Hublagen (50.1, 50.2, 50.3) des Schlüssels (50) bestimmen,

und dass der Schieber (20) axial federbelastet (40) ist und dadurch auf den eingesteckten Schlüssel (50) ausgeübte Rückstellkraft (41) erzeugt,

und dass der Schieber (20) in seiner die Mittellage (50.2) des Schlüssels (50) bestimmenden mittleren Axialposition (50.2) von einem federnden Riegel (30) eines Richtgesperres festgehalten wird und dieses Richtgesperre mittelbar, über den Schieber (20), auf den Schlüssel (50) wirkt.

- 12.) Vorrichtung nach Anspruch 11, dadurch gekennzeichnet, dass der Schieber (20) sowohl in der Anfangslage (50.1) des eingesteckten Schlüssels (50) als auch bei herausgezogenem Schlüssel sich in der gleichen Ausgangsposition (20.1) im Gehäuse (10) der Aufnahme (11) befindet.

und dass die Ausgangsposition (50.1) durch die auf den Schieber (20) wirkende axiale Federkraft (41) einerseits und einen Endanschlag (42) im Gehäuse (10) der Aufnahme (11) andererseits bestimmt ist.

- 13.) Vorrichtung nach Anspruch 12, dadurch gekennzeichnet, dass die Abdeckung (14) für die Öffnung (13) der Aufnahme (11) ihrerseits zwischen zwei Stellungen (14.1, 14.2) im Schieber (20) axial verschieblich ist,

dass diese beiden Stellungen (14.1, 14.2) durch einen vorderen und einen hinteren Endanschlag (22, 29) im Schieber (20) bestimmt sind,

dass die Abdeck-Federbelastung (15) bestrebt ist, die Abdeckung (14) axial gegen den vorderen Endanschlag (22) zu drücken,

und dass der vordere Endanschlag (22) und die Abdeck-Federbelastung (15) die bei herausgezogenem Schlüssel (50) sich ergebende abdeckwirksame Ausschubstellung (14.1) der Abdeckung (14) an der Öffnung (13) bestimmen.

- 14.) Vorrichtung nach Anspruch 13, dadurch gekennzeichnet, dass bei eingestecktem Schlüssel (50) die Abdeckung (14) sich in einer durch den hinteren Endanschlag (29) am Schieber (20) bestimmten Einschubstellung (14.2) befindet

und dass diese Einschubstellung (14.2) der Abdeckung (14) in allen drei axialen Hublagen des Schlüssels (50) vorliegt.

- 15.) Vorrichtung nach einem der Ansprüche 11 bis 14, dadurch gekennzeichnet, dass die gleichen Halteelemente (21, 22, 55), welche die kraftschlüssige Verbindung zwischen dem Schlüssel (50) und dem Schieber (20) erzeugen,

auch bei der formschlüssige Verbindung zwischen dem Schlüssel (50) und dem Schieber (20) beteiligt sind.

- 16.) Vorrichtung nach Anspruch 15, dadurch gekennzeichnet, dass die am Schieber (20) befindlichen kraftschlüssigen Halteelemente (21, 22) einen federnden Vorsprung (22) aufweisen

dass dem Vorsprung (22) ein Gegenvorsprung (23) auf seiner dem Gehäuse (10) der Aufnahme (11) zugekehrten Rückseite zugeordnet ist,

dass dieser Gegenvorsprung (23) in der die Haltelage (50.1) des Schlüssels (50) kennzeichnenden Ausgangsposition (20.1) des Schiebers (20) mit einer Aussparung (16) im Gehäuse (10) radial ausgerichtet ist, in welcher der Gegenvorsprung (23) federnd ausweicht, wenn der Schlüssel (50) eingesteckt (59) wird,

und dass dem Gegenvorsprung (23) eine radiale Stützfläche (19) im Gehäuse (10) zugeordnet ist, die das federnde Glied (22) radial versteift, wenn der Schieber (20) vom Schlüssel (50) aus seiner Ausgangsposition (20.1) in eine der tiefer gelegenen Axialpositionen (20.2, 20.3) weiterbewegt wird.

- 17.) Vorrichtung nach einem der Ansprüche 10 bis 16, dadurch gekennzeichnet, dass der axialbewegliche Schieber (20) ein mit einer Dämpfungseinrichtung (60) versehen ist,

und dass die Dämpfungseinrichtung (60) die federbedingte (40) axiale Rückbewegung (57) des im Schieber (20) aufgenommenen Schlüssels (50) aus dessen Endlage (50.3), über die Mittellage (50.2), bis zur Anfangslage (50.1) bremst.

- 18.) Vorrichtung nach einem der Ansprüche 1 bis 17, dadurch gekennzeichnet, dass die zur Unterscheidung der ausgewählten Funktion dienende Steuereinheit auch auf Betätigung bzw. Nichtbetätigung weiterer Steuerglieder im Fahrzeug anspricht, wie eine Fußbremse.
- 19.) Vorrichtung nach einem der Ansprüche 1 bis 18, dadurch gekennzeichnet, dass die zur Unterscheidung der ausgewählten Funktionen dienende Steuereinheit auf eine Nicht-Betätigung weiterer Steuerglieder im Fahrzeug anspricht.
- 20.) Vorrichtung nach einem der Ansprüche 1 bis 19, dadurch gekennzeichnet, dass der für die verschiedenen Funktionen im Kraftfahrzeug dienende Betätiger einen Taster (35) umfasst

und dass die elektrische Steuereinheit die Anzahl und/oder die Reihenfolge der verschiedenen Betätigungen (36) unterscheidet und dementsprechend die ausgewählten Funktionen im Kraftfahrzeug auslöst.

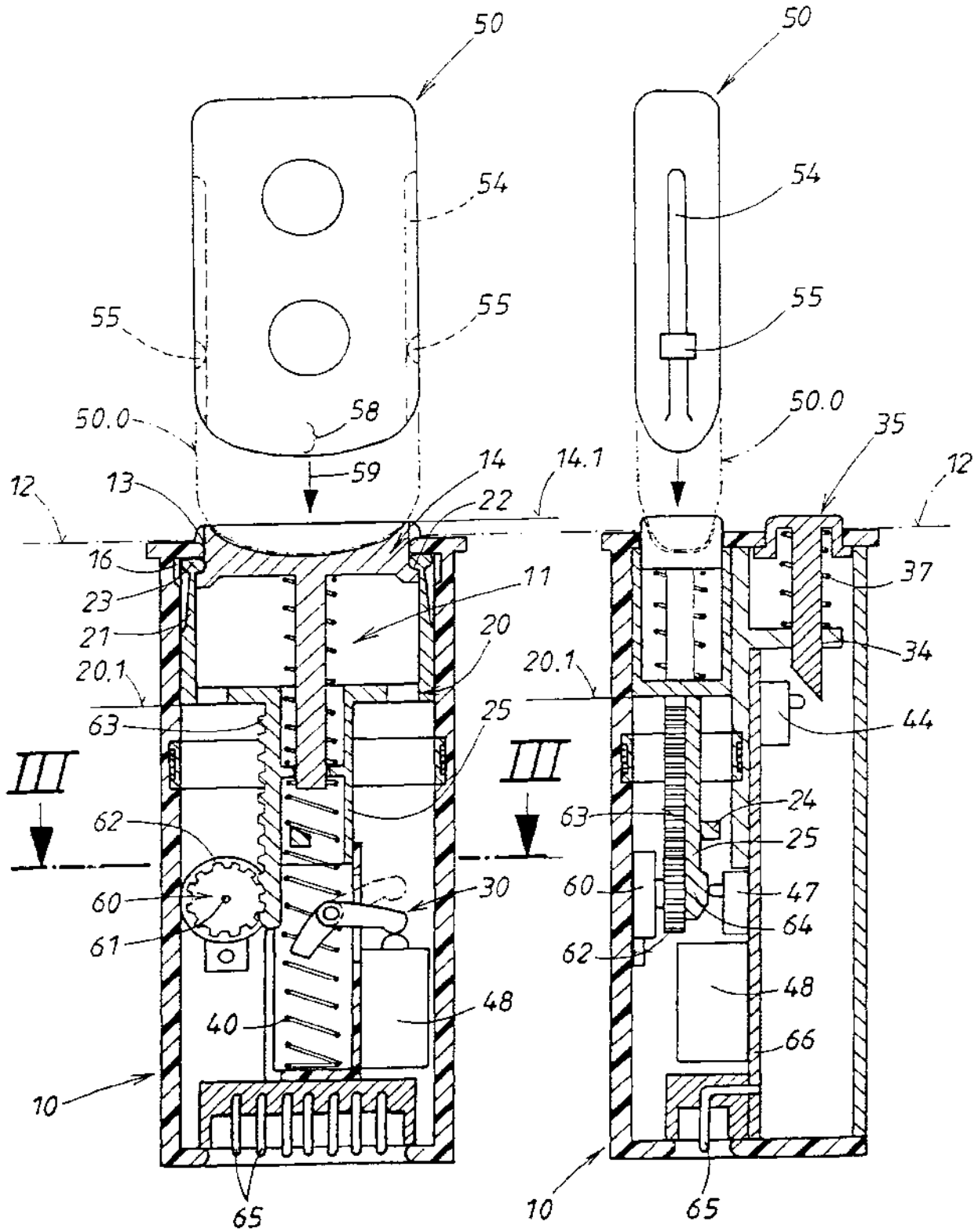


FIG. 1

FIG. 2

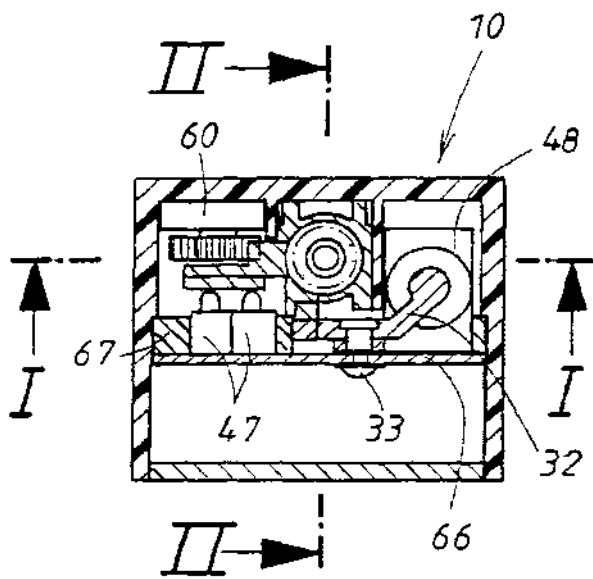


FIG. 3

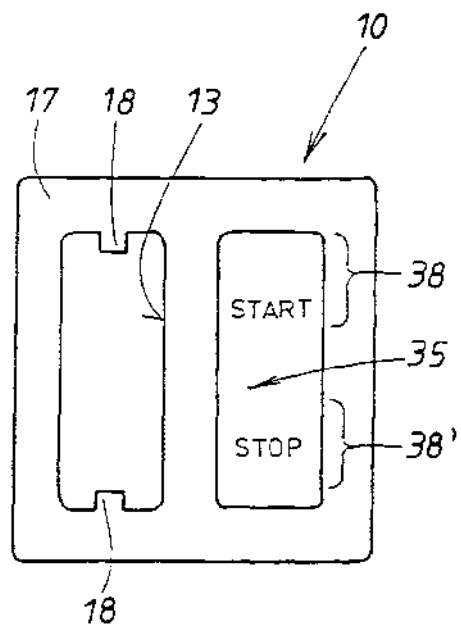


FIG. 4

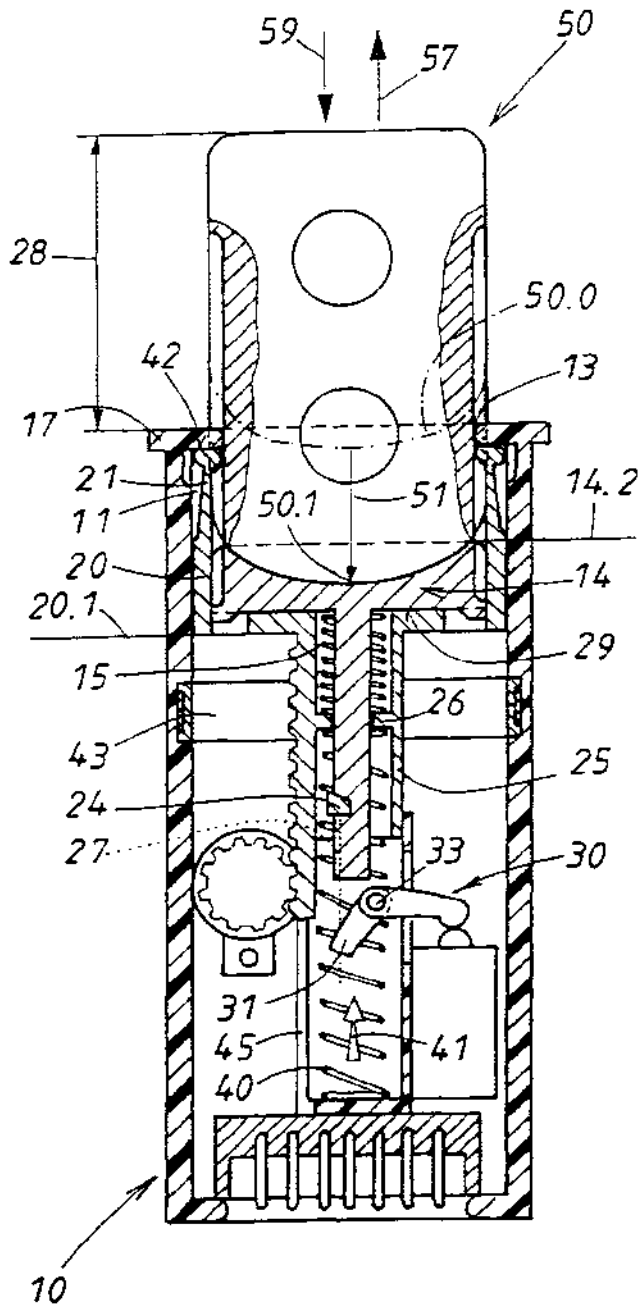


FIG. 5

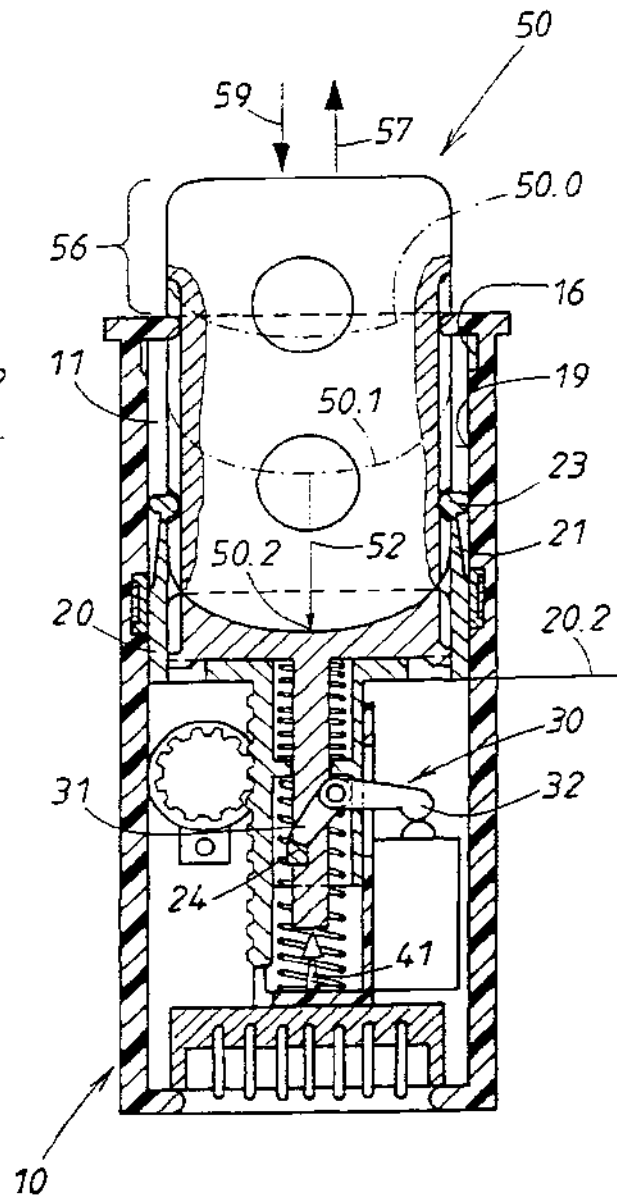


FIG. 6



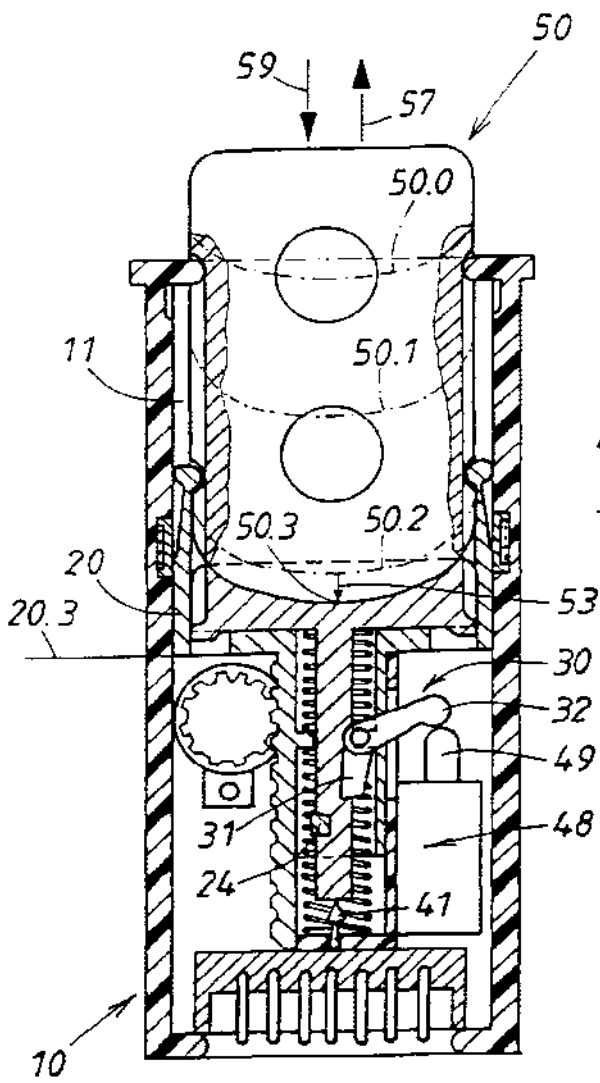


FIG. 7

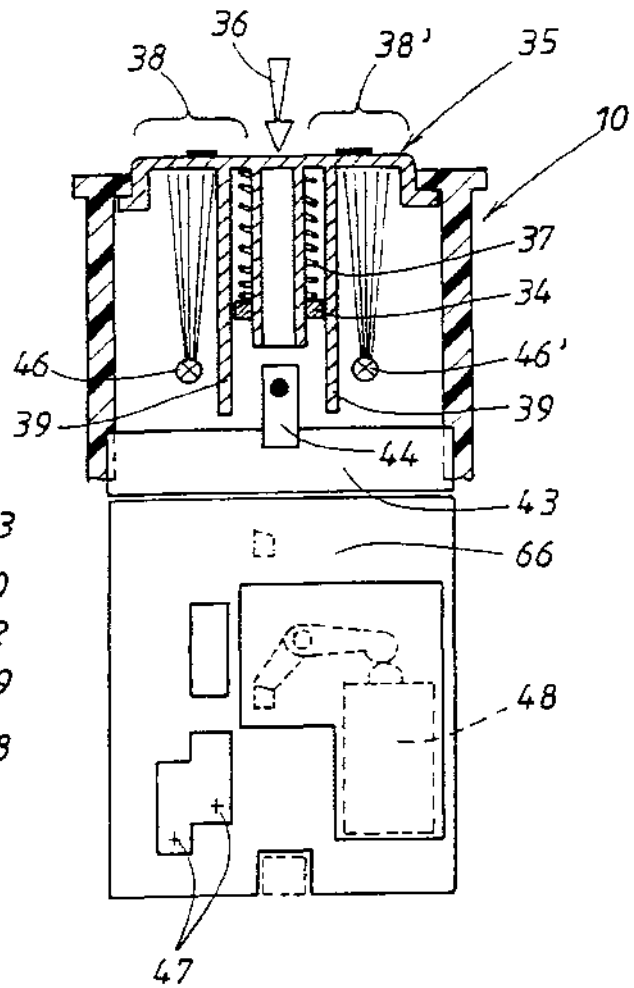


FIG. 8

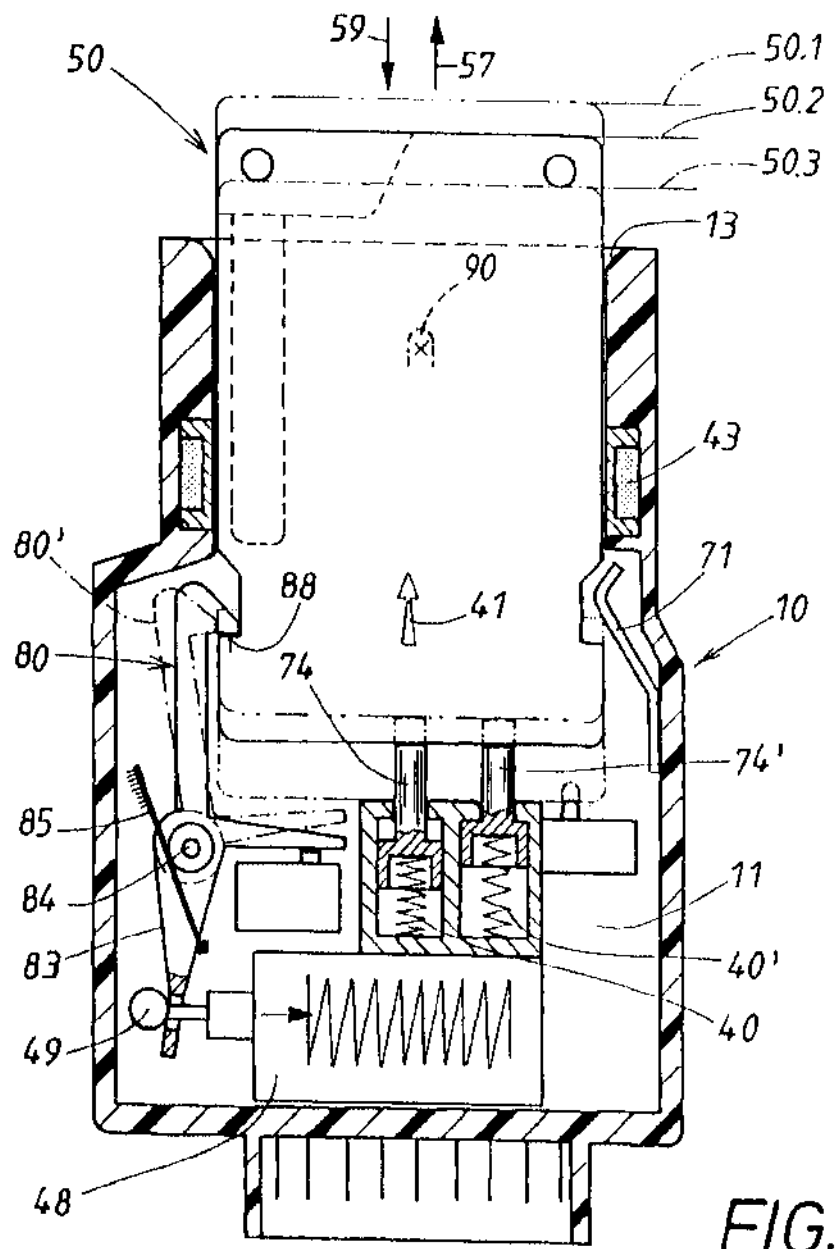


FIG. 9

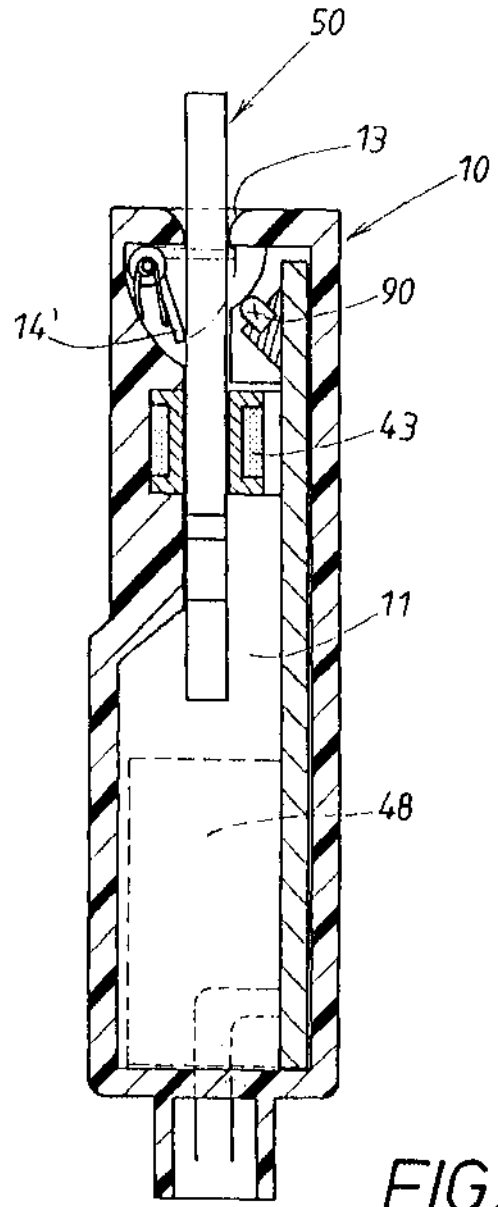


FIG. 10

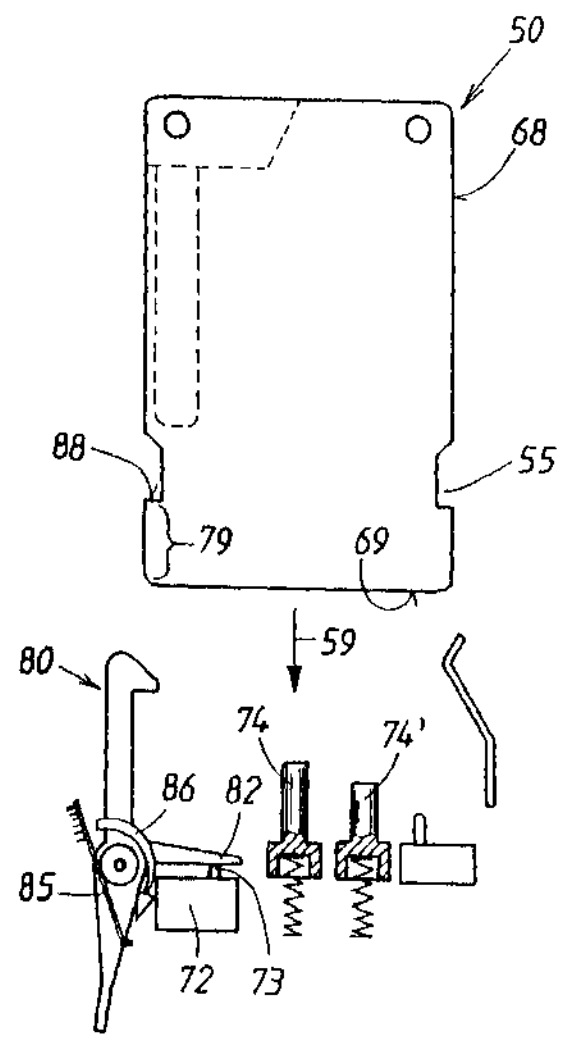


FIG. 11

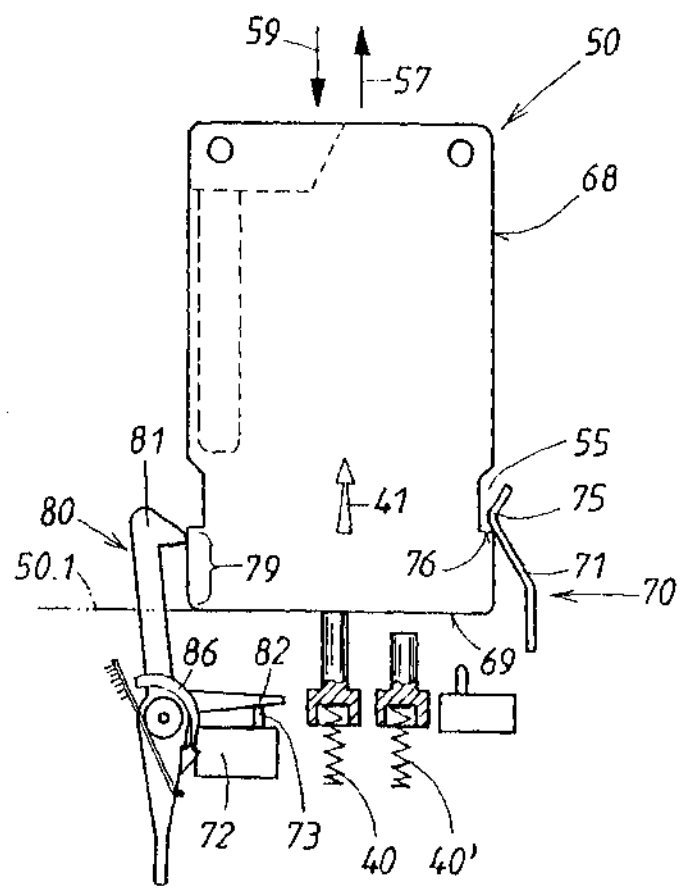


FIG. 12

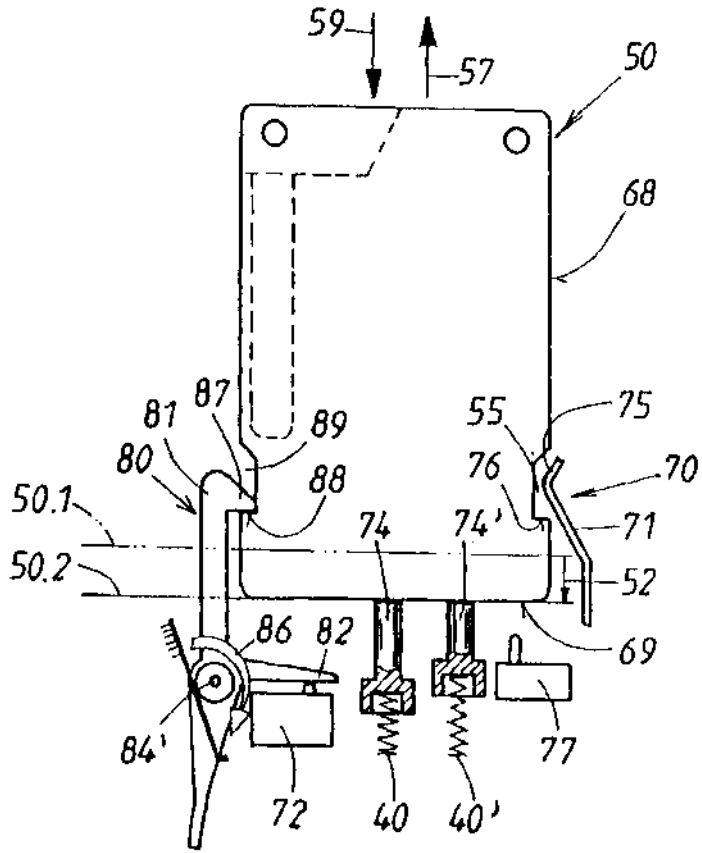


FIG. 13

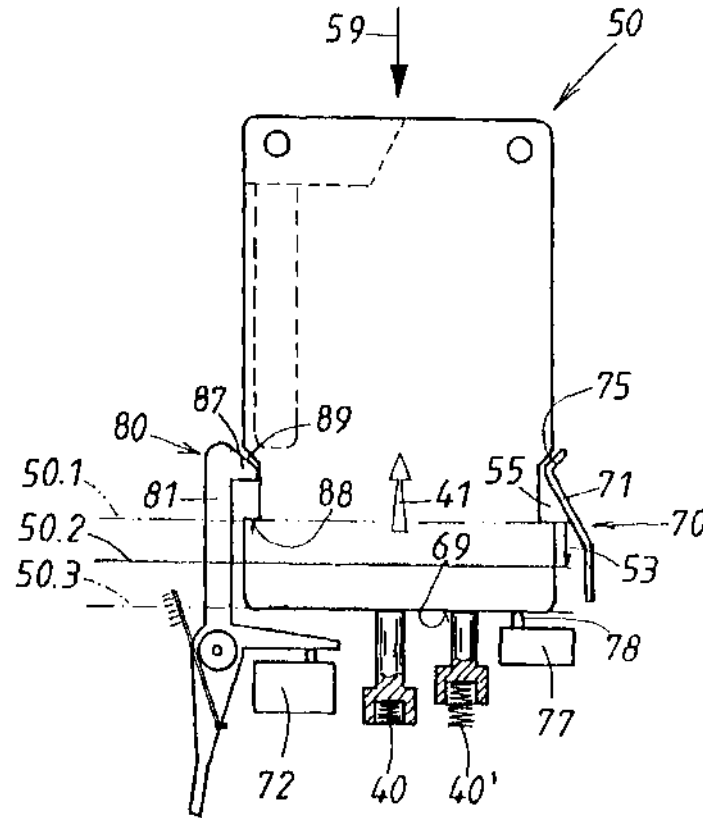


FIG. 14

# INTERNATIONAL SEARCH REPORT

Intern. Patent Application No  
PCT/EP 00/07769

<b>A. CLASSIFICATION OF SUBJECT MATTER</b> IPC 7 B60R25/04		
According to International Patent Classification (IPC) or to both national classification and IPC		
<b>B. FIELDS SEARCHED</b>		
Minimum documentation searched (classification system followed by classification symbols) IPC 7 B60R		
Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched		
Electronic data base consulted during the international search (name of data base and, where practical, search terms used) EPO-Internal, PAJ		
<b>C. DOCUMENTS CONSIDERED TO BE RELEVANT</b>		
Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	DE 33 06 863 A (DAIMLER BENZ AG) 6 September 1984 (1984-09-06) page 12, paragraph 2 -page 15, paragraph 2 figures 3-8 ---	1-4, 28 10-12 17
Y	DE 196 41 898 C (KOSTAL LEOPOLD GMBH & CO KG) 13 November 1997 (1997-11-13) column 2, line 30 - line 49; figures 1,2 ---	10, 12
Y	DE 197 47 732 A (BOSCH GMBH ROBERT) 20 May 1999 (1999-05-20) column 2, line 6 - line 14 ---	11
A	US 5 254 996 A (CLAAR KLAUS ET AL) 19 October 1993 (1993-10-19) column 5, line 25 -column 6, line 32; figures 1,2 ---	11
--- /---		
<input checked="" type="checkbox"/> Further documents are listed in the continuation of box C.		
<input checked="" type="checkbox"/> 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  <p style="text-align: center;">28 November 2000</p>	Date of mailing of the international search report  <p style="text-align: center;">04/12/2000</p>	
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040. Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer  <p style="text-align: center;">Areal Calama, A-A</p>	

# INTERNATIONAL SEARCH REPORT

Intern. Application No  
PCT/EP 00/07769

**C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P, X	WO 00 29267 A (BOSCH GMBH ROBERT ;FEUCHTER UWE (DE); GEIL ANDREAS (DE)) 25 May 2000 (2000-05-25) page 14, paragraph 4 -page 18, last paragraph; figures 1-3 -----	1, 3, 10, 11

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 00/07769

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 3306863 A	06-09-1984	NONE	
DE 19641898 C	13-11-1997	NONE	
DE 19747732 A	20-05-1999	AU 1142699 A WO 9921741 A	17-05-1999 06-05-1999
US 5254996 A	19-10-1993	DE 4038038 C EP 0492061 A ES 2061141 T JP 2053015 C JP 4273794 A JP 7044729 B	02-01-1992 01-07-1992 01-12-1994 10-05-1996 29-09-1992 15-05-1995
WO 0029267 A	25-05-2000	DE 19853075 A	25-05-2000

# INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP 00/07769

<b>A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES</b> IPK 7 B60R25/04		
Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK		
<b>B. RECHERCHIERTE GEBIETE</b>		
Recherchiertes Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole) IPK 7 B60R		
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) EPO-Internal, PAJ		
<b>C. ALS WESENTLICH ANGESEHENE UNTERLAGEN</b>		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
X	DE 33 06 863 A (DAIMLER BENZ AG) 6. September 1984 (1984-09-06)	1-4, 28
Y	Seite 12, Absatz 2 - Seite 15, Absatz 2	10-12
A	Abbildungen 3-8	17
Y	DE 196 41 898 C (KOSTAL LEOPOLD GMBH & CO KG) 13. November 1997 (1997-11-13)	10, 12
	Spalte 2, Zeile 30 - Zeile 49; Abbildungen 1, 2	
Y	DE 197 47 732 A (BOSCH GMBH ROBERT) 20. Mai 1999 (1999-05-20)	11
	Spalte 2, Zeile 6 - Zeile 14	
A	US 5 254 996 A (CLAAR KLAUS ET AL) 19. Oktober 1993 (1993-10-19)	11
	Spalte 5, Zeile 25 - Spalte 6, Zeile 32; Abbildungen 1, 2	
	-/--	
<input checked="" type="checkbox"/> Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen <input checked="" type="checkbox"/> 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 erfinderscher Tätigkeit beruhend betrachtet werden ** Veröffentlichung von besonderer Bedeutung: die beanspruchte Erfindung kann nicht als auf erfinderscher 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. November 2000		Absenddatum des internationalen Recherchenberichts 04/12/2000
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 Beauftragter Areal Calama, A-A



**INTERNATIONALER RECHERCHENBERICHT**

Internationales Aktenzeichen  
PCT/EP 00/07769

**C.(Fortsetzung) ALS WESENTLICH ANGESEHENE UNTERLAGEN**

Kategorie°	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
P, X	WO 00 29267 A (BOSCH GMBH ROBERT ; FEUCHTER UWE (DE); GEIL ANDREAS (DE)) 25. Mai 2000 (2000-05-25) Seite 14, Absatz 4 -Seite 18, letzter Absatz; Abbildungen 1-3 -----	1, 3, 10, 11

# INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Intern. Internationales Aktenzeichen

PCT/EP 00/07769

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 3306863 A	06-09-1984	KEINE	
DE 19641898 C	13-11-1997	KEINE	
DE 19747732 A	20-05-1999	AU 1142699 A WO 9921741 A	17-05-1999 06-05-1999
US 5254996 A	19-10-1993	DE 4038038 C EP 0492061 A ES 2061141 T JP 2053015 C JP 4273794 A JP 7044729 B	02-01-1992 01-07-1992 01-12-1994 10-05-1996 29-09-1992 15-05-1995
WO 0029267 A	25-05-2000	DE 19853075 A	25-05-2000

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum  
Internationales Büro



(43) Internationales Veröffentlichungsdatum  
31. Mai 2001 (31.05.2001)

PCT

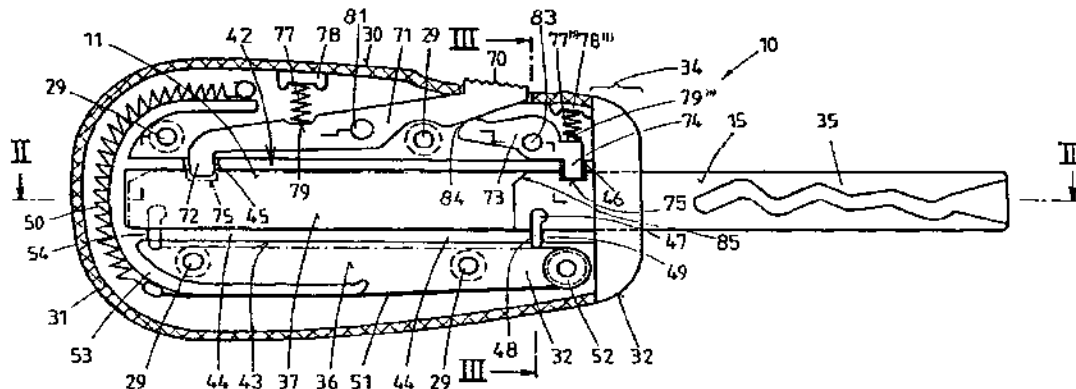
(10) Internationale Veröffentlichungsnummer  
WO 01/38673 A1

- (51) Internationale Patentklassifikation<sup>7</sup>: E05B 19/04, A45C 11/32
- (21) Internationales Aktenzeichen: PCT/EP00/11504
- (22) Internationales Anmeldedatum: 18. November 2000 (18.11.2000)
- (25) Einreichungssprache: Deutsch
- (26) Veröffentlichungssprache: Deutsch
- (30) Angaben zur Priorität: 199 56 392.6 24. November 1999 (24.11.1999) DE
- (71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von US): HUF HÜLSBECK & FÜRST GMBH & CO. KG [DE/DE]; Steeger Strasse 17, 42551 Velbert (DE).
- (72) Erfinder; und  
(75) Erfinder/Anmelder (nur für US): WITTMER, Reinhard [DE/DE]; Beuthener Strasse 26, 42579 Heiligenhaus (DE).  
BARREBERG, Günter [DE/DE]; Am Buschkothen 20, 42551 Velbert (DE).  
HABECKE, Mathias [DE/DE]; Nikolaus-Gross-Strasse 12, 45529 Hattingen (DE).  
JACOB, Dirk [DE/DE]; Breslauer Strasse 13, 42579 Heiligenhaus (DE).
- (74) Anwalt: MENTZEL, Norbert; Kleiner Werth 34, 42275 Wuppertal (DE).
- (81) Bestimmungsstaaten (national): AU, BR, CN, IN, JP, KR, US.
- (84) Bestimmungsstaaten (regional): europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).

[Fortsetzung auf der nächsten Seite]

(54) Title: KEY, IN PARTICULAR FOR A MOTOR VEHICLE

(54) Bezeichnung: SCHLÜSSEL, INSBESONDERE FÜR KFZ



(57) Abstract: The invention relates to a key, in particular for a motor vehicle, comprising a housing (30) and a mechanical key part (35) connected thereto. In keys of this type, the locking element of the key part is usually converted from an inoperative position (11) into a working position (15), in which the key (10) can be used to mechanically operate a lock or a locking cylinder, by means of a mechanism (47, 50, 51, 52, 60, 61, 62, 64, 65, 66) which is located in the housing. In order to improve a key of this type, the invention proposes the provision of a traction or force of pressure regulator (50) for the mechanism (47, 50, 51, 52, 60, 61, 62, 64, 65, 66) which acts indirectly upon the actuator (47) via traction or thrust means (51).

(57) Zusammenfassung: Die Erfindung betrifft einen Schlüssel, insbesondere für Kfz mit einem Gehäuseteil (30) und einem daran angeordneten mechanischen Schlüsselteil (35). Bei solchen Schlüsseln ist es bekannt, den schliesswirksamen Teil des Schlüsselteils mittels einer Mimik (47, 50, 51, 52, 60, 61, 62, 64, 65, 66), welche im Gehäuse angeordnet ist, von einer Ruhestellung (11) in eine Arbeitsstellung (15) zu überführen, in der der Schlüssel (10) zur mechanischen Betätigung eines Schlosses oder Schliesszylinders benutzt werden kann. Zur Verbesserung eines derartigen Schlüssels wird vorgeschlagen, dass die Mimik (47, 50, 51, 52, 60, 61, 62, 64, 65, 66) einen Zug- (50) oder Druckkraftspeicher umfasst, der indirekt über ein Zug- (51) oder Schubmittel an dem Stellglied (47) angreift.

WO 01/38673 A1



**Veröffentlicht:**

- Mit internationalem Recherchenbericht.
- Vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen.

*Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.*

### Schlüssel, insbesondere für Kfz

Die Erfindung richtet sich auf einen Schlüssel der in Anspruch 1 genannten Art. Derartige Schlüssel kommen insbesondere bei Kraftfahrzeugen zur Anwendung.

Aus der US 2,690,666, als nächstliegenden Stand der Technik, ist ein Schlüsselhalter bekannt, bei dem in einem Gehäuse befindliche Schlüssel über ihnen zugeordnete Druckfedern aus dem Gehäuse herausbewegt werden können. Bei diesem Schlüsselhalter kann jeweils ein Schlüssel über einen Wahlschalter ausgewählt werden, und der Schlüssel dann durch Betätigung eines Auslösemittels freigegeben werden. Der ausgewählte Schlüssel wird daraufhin von der Kraft der Druckfeder aus dem Gehäuse heraus in seine Arbeitsstellung überführt. Die Federn greifen bei dem Gegenstand der US-Schrift direkt am hinteren Ende der Schlüssel an, so daß sie in der Ruhestellung des Schlüssels im Gehäuseinnenraum einen erheblichen Teil der Baulänge des Schlüsselgehäuses einnehmen. Eine erhöhte Baulänge ist jedoch insbesondere bei Kfz-Schlüsseln nicht wünschenswert, die während des Betriebes eines Kfz in dessen Zündschloß verbleiben, da durch die in

den Bewegungsraum eines Knies hineinragenden Schlüssel das Verletzungsrisiko im Bereich des rechten Knies einer Fahrerin oder eines Fahrers erhöht wird.

Aus der US 2,550,375 ist ebenfalls ein in einem Gehäuse lateral verschieblich angeordneter Schlüssel bekannt. Auch bei diesem Schlüssel ist im rückwärtigen Bauraum des Schlüssels ein Federglied angeordnet, welches direkt auf den Schlüssel einwirkt. Das Federglied ist hier jedoch als Zugfeder ausgeführt, welches den Schlüssel von seiner ausgeschobenen Lage in seine eingezogene Position automatisch zurückfährt, wenn eine Auslösetaste betätigt wird, die den Schlüssel freigibt.

Aus der DE-GM 17 13 197 ist ein Schlüsselgehäuse bekannt, bei dem ein darin liegender Schlüssel über eine manuelle Betätigung aus dem Gehäuse heraus oder in das Gehäuse hineingeschoben werden kann. Die Betätigung des Schlüssels über eine auf diesen einwirkende Mimik ist dieser Schrift nicht zu entnehmen. Der in dem Gehäuse befindliche Schlüssel kann lediglich über ein oder mehrere Federelemente in seiner im Gehäuse eingezogenen oder aus dem Gehäuse herausgeschobenen Stellung fixiert werden.

Bei einem von der Firma Huf gefertigten Elektronischen-Mechanischen-Schlüssel ist es bekannt, einen mechanischen Schlüsselteil aus- und einklappbar an einem Schlüsselgehäuse anzuordnen. Bei diesem Schlüssel ist die Schlüsselelektronik in einem ersten Gehäuseteil und der mechanische Schlüsselteil in und an einem zweiten Gehäuseteil angeordnet. Die Schnittstellen zwischen dem ersten und dem zweiten Gehäuseteil sind bei diesem Schlüssel sehr verwinkelt und maßlich kompliziert.

Der mechanische Schlüsselteil liegt im eingeklappten Zustand an einer Längsseite des Schlüsselgehäuses, innerhalb einer Eintiefung, die als Schlüsselaufnahme dient.

Der Schlüssel ist in der Aufnahme des Gehäuses an seiner in Ausklapprichtung liegenden Seite offen zugänglich.

Außen an dem Schlüssel ist eine Auslösetaste angeordnet, über deren Betätigung der Schlüssel von seiner Ruhestellung am Gehäuse in eine Arbeitsstellung ausgeklappt werden kann, in der das mechanische Schlüsselteil z.B. zur Betätigung eines Schließzylinders oder eines Zündschlosses benutzt werden kann. Der Ausklappvorgang geschieht nach Betätigen der Auslösetaste automatisch über einen im Schlüsselgehäuse angeordneten Federtrieb der auf den mechanischen Schlüsselteil wirkt.

Zum Einklappen des mechanischen Schlüsselteils muss erneut die Auslösetaste gedrückt werden und der Schlüssel dann manuell wieder in seine Ruhestellung in der seitlich am Gehäuse angeordneten Aufnahme eingeklappt werden.

Von Nachteil bei einem derartigen Schlüssel ist es, dass sich an dem in der Aufnahme offen zugänglichen Schlüssel Dreckpartikel sammeln, die über den mechanischen Schlüsselteil in den zu betätigenden Schließzylinder und/oder des Zündschloss etc. gelangen und diese dadurch auf Dauer verschmutzen und gegebenenfalls funktionsuntüchtig werden können. Auch ist die Öffnung in die der Schlüssel einklappen kann optisch unschön.

Aus der DE 296 18 616 U1 ist ein Kraftfahrzeugschlüssel bekannt, der ebenfalls über eine Mimik von einer an einer Gehäuseseite angeklappten Lage in eine aus dem Gehäuse herausstehende, ausgeklappte Arbeitslage überführbar ist.

Aufgabe der vorliegenden Erfindung ist es, einen Schlüssel bereitzustellen, der einen verhältnismäßig kurzen Bauraum aufweist und der ein gutes optisches Erscheinungsbild aufweist.

Dieses wird erfindungsgemäß durch die im Anspruch 1 genannten Maßnahmen erreicht, denen folgende besondere Bedeutung zukommt. Zur Lösung der patentgemäßen Aufgabe wird vorgeschlagen, das Schlüsselteil in seiner Ruhestellung innen im Gehäuse anzuordnen, wobei das Schlüsselteil nach Betätigung der Auslösetaste über eine in dem Gehäuse angeordnete Mimik von seiner Ruhestellung im Inneren des Gehäuses durch eine Längsverschiebung in seine Arbeitsstellung überführt wird, in der zumindest der schließwirksame Teil des mechanischen Schlüsselteils außerhalb des Gehäuses liegt. Hierzu weist die Mimik einen Zug- oder Druckkraftspeicher auf, der indirekt über ein Zug- oder Schubmittel an dem Stellglied des Schlüsselteils angreift. Durch diese Maßnahmen ist es nicht mehr notwendig, den Zug- oder Druckkraftspeicher in unmittelbarer Nachbarschaft zum mechanischen Schlüsselteil anzuordnen, um das Bewegungsmoment vom Zug- oder Druckkraftspeicher auf das mechanische Schlüsselteil zu übertragen. Vielmehr wird es möglich, den Zug- oder Druckkraftspeicher an jeder beliebigen Position im Schlüsselgehäuse anzuordnen. So kann der Zug- oder Druckkraftspeicher insbesondere auch seitlich, neben dem im Gehäuse eingezogenen Schlüssel angeordnet werden. Der Bauraum, insbesondere die Bauraumlänge des Schlüsselgehäuses kann hierdurch vermindert werden. Ebenfalls wird eine größere Variationsbreite bei der Formgestaltung des Schlüsselgehäuses ermöglicht. Der Zugkraftspeicher könnte z.B. eine zugbelastete Feder, ein Gummielement, eine Unterdruckkammer, ein Solenoid etc. sein. Als Druckkraftspeicher können z.B. vorgesehen sein linear wirkende Druckfedern, Spiralfedern, elastische Elemente (z.B. aus Kunststoff), Druckkörper, Solenoide etc.

Bei der indirekten Übertragung der Verstellbewegung vom Druckkraftspeicher auf das mechanische Schlüsselteil kann das Schubmittel z.B. ein Treibriemen, eine Stellkette, ein Stellband, ein Zahnriemen, ein Zahnrad etc. sein.



Um ein reibungsloses Herausfahren des mechanischen Schlüsselteils zu gewährleisten, sind im Innenraum des Gehäuses Mittel angeordnet, durch die das Schlüsselteil bei der Längsbewegung von seiner Ruhestellung in seine Arbeitsstellung geführt ist.

Ein weiterer Vorteil der sich aus der erfindungsgemäßen Lösung gemäß Anspruch 1 ergibt ist der, dass an dem Schlüsselgehäuse nunmehr glatte Flächen überwiegen und keine vorstehenden Kanten und unschöne Vertiefungen mehr vorhanden sind, so dass der Schlüssel eine sehr ansprechende Optik aufweist.

Außerdem ist die Bedienungsfreundlichkeit durch das automatische Ausfahren des mechanischen Schlüsselteils und dem einfach zu bewirkenden Wiedereinschieben desselben verbessert worden.

Vorteilhaft nach Anspruch 2 kann es auch sein, wenn die Schlüsselöffnung im Gehäuseteil im wesentlichen formschlüssig zur Außenkontur des mechanischen Schlüsselteils ausgeführt ist, so dass möglichst wenig Öffnungsraum zwischen Gehäusewand und Schlüsselteil vorhanden ist, an dem Schmutzpartikel in das Gehäuseinnere eindringen können. Ferner wird durch die formschlüssige Ausführung der Öffnung ein Abstreifen von eventuell während oder nach der Betätigung aufgefangenen Schmutzpartikeln ermöglicht.

In einer weiteren günstigen Ausführungsform der Erfindung kann gemäß Anspruch 3 auch ein Mittel zum Verschließen der Schlüsselöffnung, wie etwa eine Klappe oder ein Schieber, der manuell oder automatisch betätigt wird, vorgesehen sein, der das Gehäuseteil in der Ruhestellung des darin angeordneten mechanischen Schlüsselteils gegen ein Eindringen von Schmutz gänzlich abriegelt.

Vorteilhaft gemäß Anspruch 4 kann es sein, wenn das Schlüsselteil innerhalb des Gehäuseteils in einem Führungskanal liegt, innerhalb dessen das Schlüsselteil bei

seiner Längsverschiebung geführt ist. Günstigerweise können zur Erzeugung des Führungskanals auch umgebende Gehäusewände wie z.B. die an den Flächenseiten des umgebenden Gehäuseteils liegenden Wände zur Ausbildung des Führungskanals herangezogen werden.

Der Führungskanal kann eine seitliche Öffnung aufweisen, durch den ein Stellglied, wie etwa ein Zahnrad oder ein Mitnehmerzapfen, auf das mechanische Schlüsselteil einwirken kann und derart eine von der Mimik ausgeübte Verstellbewegung auf das mechanische Schlüsselteil überträgt.

Günstig kann es auch sein, wenn Rastmittel vorgesehen sind, die das mechanische Schlüsselteil in seiner Ruhe- und in seine Arbeitsstellung im wesentlichen bewegungsstarr halten. Nach Betätigung der Auslösetaste oder eines anderen Auslösemittels geben die Rastmittel das mechanische Schließteil frei, so dass diese von der einen Stellung in die andere Stellung verfahrbar ist. Die Rastmittel können z.B. an einem oder mehreren Hebeln angeordnete Haken umfassen, die in der Raststellung in eine am Umfang des Schließteils befindliche Aussparung eingreifen, oder die in einem Vorsprung, einer Nase, einem Gegenrastglied etc. eines zur Mimik gehörenden Stellmittels angreifen und derart indirekt das mechanische Schließteil in seiner Arbeits- oder Ruhestellung halten.

Bei der Verwendung eines Zugkraftspeichers kann es günstig sein, wenn der Zugweg des Zugkraftspeichers und/oder des durch den Zugkraftspeichers betätigten Zugmittels durch ein- oder mehrfache Umlenkung des Zugkraftspeichers und/oder des Zugmittels an einem oder mehreren Umlenkteilen, wie z.B. Umlenkrollen oder Umlenkstegen vergrößert ist. Durch diese Maßnahme wird ein weitgehendes Herausfahren des mechanischen Schließteils bei der Überführung von seiner Ruhestellung in seine Arbeitsstellung erreicht.

Es kann ferner vorteilhaft sein, die Schlüsselelektronik und die Schlüsselmechanik in zwei, in sich abgeschlossenen Gehäuseteilen anzuordnen, die beide entlang ebener Verbindungsflächen lösbar aneinander festgelegt sind. Günstigerweise ist der Batteriedeckel derart an dem Gehäuseteil angeordnet das die Schlüsselelektronik aufweist, dass er durch das gegenüberliegende Gehäuseteil mit der Mechanik darin verdeckt wird. Zum Wechseln der Batterie muss also lediglich eine Trennung der beiden Gehäuseteile voneinander vorgenommen werden um danach den Batteriedeckel öffnen zu können. Zur Verbindung der beiden Gehäuseteile sind die verschiedensten Verbindungsmittel denkbar. So können z.B. Schwalbenschwanznuten oder -vertiefungen und Schwalbenschwanzvorsprünge - oder -erhöhungen an den Gehäuseteilen angeordnet sein, die ineinandergeschoben die Verbindung der beiden Gehäuseteile gewährleisten.

Weitere Vorteile und Maßnahmen der Erfindung ergeben sich aus den Unteransprüchen, der nachfolgenden Beschreibung und den Zeichnungen. In den Zeichnungen ist die Erfindung in drei Ausführungsbeispielen dargestellt. Es zeigen:

- Fig. 1        schematisch eine erste Ausführungsform eines erfindungsgemäßen Schlüssels im Schnitt durch das zweite, die Mechanik enthaltene Gehäuseteil,
- Fig. 2        schematisch, die erste Ausführungsform eines erfindungsgemäßen Schlüssels im Schnitt gemäß II - II aus Fig. 1,
- Fig. 3        schematisch, die erste Ausführungsform des erfindungsgemäßen Schlüssels im Schnitt gemäß III - III aus Fig. 1,

- Fig. 4 schematisch, das erste Gehäuseteil der ersten Ausführungsform des erfindungsgemäßen Schlüssels mit der Schlüsselektronik gemäß dem Schnitt IV - IV aus Fig. 2,
- Fig. 5 schematisch, das zweite Gehäuseteil der ersten Ausführungsform des erfindungsgemäßen Schlüssels mit dem mechanischen Schlüssel im Schnitt gemäß V - V aus Fig. 2,
- Fig. 6 schematisch, die erste Ausführungsform des erfindungsgemäßen Schlüssels in Seitenansicht, bei dem beide Gehäuseteile aneinander festgelegt sind,
- Fig. 7 schematisch, die erste Ausführungsform des erfindungsgemäßen Schlüssels, bei dem die Verbindungsmittel der beiden Gehäuseteile gelöst sind,
- Fig. 8 schematisch, die erste Ausführungsform des erfindungsgemäßen Schlüssels in einem Schnitt entlang VIII - VIII aus Fig. 6,
- Fig. 9 schematisch, ein zweites Ausführungsbeispiel eines erfindungsgemäßen Schlüssels, in einem Schnitt durch das zweite Gehäuseteil mit der Schlüsselmechanik,
- Fig. 10 schematisch, die zweite Ausführungsform des erfindungsgemäßen Schlüssels im Schnitt gemäß X - X aus Fig. 9,
- Fig. 11 schematisch, eine dritte Ausführungsform des erfindungsgemäßen Schlüssels im Schnitt durch das die

Mechanik aufweisende zweite Gehäuseteil, in der Ruhestellung des mechanischen Schlüsselteils,

Fig. 12 schematisch, die dritte Ausführungsform des erfindungsgemäßen Schlüssels gemäß Fig. 11 in der Arbeitsstellung des mechanischen Schlüsselteils.

In den Fig. 1 bis 8 ist eine erste Ausführungsform des erfindungsgemäßen Schlüssels 10 dargestellt. Bei dieser Ausführungsform setzt sich der Schlüssel zusammen aus einem ersten Gehäuseteil 20 und einem zweiten Gehäuseteil 30. Das erste Gehäuseteil umfasst eine Gehäusegrundplatte 22 und einen Gehäusedeckel 21. In dem Gehäusedeckel 21 sind Tastfelder 26 angeordnet, über die eine im Inneren des ersten Gehäuseteiles 20 liegende Elektronik 25 betätigt werden kann. In der Gehäusegrundplatte 22 ist ein Batteriefachdeckel 23 angeordnet, über den eine Batterie 24, die der Stromversorgung der Elektronik 25 dient, in das Gehäuseteil 20 ein- und ausgeführt werden kann. Das erste Gehäuseteil 20 ist wasserdicht verschlossen, wobei der Gehäusedeckel 21 an der Gehäusegrundplatte 22 über Schraubmittel 29 festgelegt ist. An dem Schlüssel 10 ist in diesem Ausführungsbeispiel noch eine Öse 19 vorgesehen, an die z.B. ein Schlüsselanhänger angebracht werden kann.

An dem ersten Gehäuseteil 20 ist entlang einer planaren Ebene 14 ein zweites Gehäuseteil 30 angeordnet. Das zweite Gehäuseteil 30 besteht in diesem Ausführungsbeispiel ebenfalls aus einer Gehäusegrundplatte 32 und einem diese abdeckenden Gehäusedeckel 31. Beide Gehäuseteile 20 und 30 sind über Verbindungsmittel 28, 33 lösbar miteinander verbunden. Bei diesen Verbindungsmitteln handelt es sich in diesem Ausführungsbeispiel um Verrastmittelvorsprünge 28, die in Nuten 27 in der Gehäusegrundplatte 32 des ersten Gehäuseteiles 20 angeordnet sind und auf Seiten des zweiten Gehäuseteiles 30 um Schwalbenschwanzzapfen 33, die an der Gehäusegrundplatte 32 angeformt

sind. Um beide Gehäuseteile 20, 30 voneinander zu lösen, z.B. zum Zwecke des Austausches der Batterie 23, werden beide Gehäuseteile in Demontagerichtung 17 (Fig. 7) gegeneinander verschoben, wobei ein Anfangswiderstand zu überwinden sein kann. Die Schwalbenschwanzzapfen 33 befinden sich nach dieser Verschiebung gemäß Pfeil 17 in dem offenen Teil der Nut 27, so dass nun beide Gehäuseteile 20, 30 voneinander getrennt werden können. Zur Montage müssen die beiden Gehäuseteile 20 und 30 in entsprechender Weise aneinandergesetzt werden, wobei die Schwalbenschwanzzapfen 33 in die Nut 27 an dem gegenüberliegenden Gehäuseteil eingeführt werden müssen, und das Gehäuseteil 20 daraufhin in Montagerichtung 18 (Fig. 7) gegenüber dem Gehäuseteil 30 verschoben werden. Die Schwalbenschwanzzapfen 33 verhaken sich dabei hinter dem Verrastmittelvorsprung 28 in der Gehäusegrundplatte 22 des ersten Gehäuseteiles, wodurch beide Gehäuseteile 20, 30 aneinander festgelegt werden. Durch das Festlegen der beiden Gehäuseteile entlang einer Ebene wird die vorbeschriebene Montage/Demontage vereinfacht.

In dem zweiten Gehäuseteil 30 ist eine Schlüsselmechanik angeordnet, über die ein mechanisches Schlüsselteil 35, welches sich in einer Ruhestellung 11 im Gehäuseinnenraum 36 des zweiten Gehäuseteils 30 befindet, durch Betätigung eines Auslösemittels, wie etwa einer Auslösetaste 70 automatisch in eine Arbeitsstellung 15 verfahren werden kann, in der das mechanische Schlüsselteil 35 zur Betätigung eines Schließzylinders oder eines Zündschlosses etc. verwendet werden kann. Das mechanische Schlüsselteil 35 ist dazu in dem vorliegenden Ausführungsbeispiel gemäß den Fig. 1 bis 8 wie folgt in dem zweiten Gehäuseteil 30 angeordnet.

Im Gehäuseinnenraum 36 des zweiten Gehäuseteils 30 ist ein Führungskanal 37 angeordnet, dessen beide Flächenwände 40 und 41 aus den Flächenseiten 38 und 39 der angrenzenden Gehäusegrundplatte 32 und des Gehäusedeckels 31 gebildet wird. Der Führungskanal 37 wird weiterhin zu seinen beiden Seiten von den Wänden 42 und 43 begrenzt. In dem Führungskanal 37 ist das mechanische Schlüsselteil 35

verschiebbar angeordnet. Dieser Führungskanal 37 ist an seinem vorderen Ende mit einer Schlüsselöffnung 12 versehen, durch die das mechanische Schlüsselteil 35 aus dem Gehäuseteil 20 heraus in seiner Arbeitsstellung 15 gelangen kann. In seinem hinteren Bereich ist der Führungskanal 37 in diesem Ausführungsbeispiel durch eine Führungswand 53 abgeschlossen. An der, der Wand 42 zugewandten Schmalseite des mechanischen Schlüsselteils 35 ist eine Aussparung 75 im hinteren Bereich des mechanischen Schlüsselteils 35 angeordnet. In dieser Aussparung 75 greift in der Ruhestellung 11 der Rasthaken 72 eines Hebels 71, durch den das mechanische Schlüsselteil 35 in der Ruhestellung 11 gehalten wird. Der Rasthaken 72 wird dabei mit der Kraft eines Druckmittels 77, wie etwa einer Feder, die an der Ansatzstelle 79 am Hebel 71 angreift und die anderenends in einem Federsitz 78 an der Wand des Gehäusedeckels 31 abgestützt ist, in der Aussparung 75 gehalten. Der Hebel 71 ist an einer Achse 81 schwenkbar gelagert. Der Hebel 71 ist über eine Auslösetaste 70, die in diesem Ausführungsbeispiel an den Hebel 71 angeformt ist, zu betätigen, wodurch der Rasthaken 72 aus der Aussparung 75 ausrastet, wenn das mechanische Schlüsselteil 35 in seiner Ruhestellung 11 sitzt.

Damit der Rasthaken 72 die Wand 42 durchgreifen kann, um in die Aussparung 75 im mechanischen Schlüsselteil 35 einzugreifen, ist in der Wand 42 eine Öffnung 45 vorgesehen.

Im vorderen Bereich des Schlüssels 10 unmittelbar hinter einem Frontteil 34 der Gehäusegrundplatte, in welcher die Schlüsselöffnung 12 sitzt, ist ein zweiter Hebel 73 angeordnet, der um eine Achse 83 verschwenkbar ist, und der einen Rasthaken 74 aufweist, der in der Arbeitsstellung 15 des mechanischen Schlüsselteils 35 in die Aussparung 75 im mechanischen Schlüsselteil 35 eingreift. In der Wand 42 des Führungskanals 37 ist wiederum eine Öffnung 46 vorgesehen, die ein Durchgreifen der Wand 42 durch den Rasthaken 74 erlaubt. Der Rasthaken 74 wird wiederum mittels der Kraft einer Feder 79<sup>''''</sup>, die an den Ansatzstellen 77<sup>''''</sup> und 78<sup>''''</sup> zwischen dem Hebel 73 und der Wand 42 des Gehäuseteils 31 festgelegt ist. Der

Hebel 73 steht an der Berührungsstelle 84 in mechanischem Kontakt mit dem Hebel 71. Bei einer Betätigung der Auslösetaste 70 wird hierdurch, neben dem Hebel 71, auch der Hebel 73 betätigt und der Rasthaken 74 aus dem Führungskanal 37 und gegebenenfalls aus der Aussparung 75 herausgezogen, wenn das mechanische Schlüsselteil 35 in seiner Arbeitsstellung 15 sitzt. Der aus den Hebeln 71 und 73 gebildete Doppelhebel ermöglicht es, dass an dem mechanischen Schlüsselteil nur eine Aussparung 75 am Ende des Schaftes des Schlüsselteils erforderlich ist.

Das mechanische Schlüsselteil 35 kann über eine Mimik nach Betätigung der Auslösetaste 70 automatisch aus seiner Ruhestellung 11 in die Arbeitsstellung 15 überführt werden. Hierzu ist in dem vorliegenden Ausführungsbeispiel zunächst ein Zugkraftspeicher 50 in Form einer Zugfeder vorgesehen, die im hinteren Bereich des Gehäuseteils 30 angeordnet ist. Die Feder 50 ist mit einem Zugmittel 51 wie etwa einem Kunststoffstrang oder Kunststoffband verbunden, wobei die Feder 50 und Zugmittel 51 im hinteren Bereich des Gehäuseteils 30 entlang der Führungswand 53 geführt sind. Das Zugmittel 51 ist andernends wiederum an einem Stellglied 47 festgelegt, welches seinerseits fest verbunden mit dem mechanischen Schlüsselteil 35 ist, welches im hinteren Bereich des Schlüsselteils 35 angeordnet ist. Das Zugmittel 51 ist im vorderen Bereich des Gehäuseteils 30 um eine Umlenkrolle 52 herumgeführt, so dass der Zugweg der Feder 50 und des Zugmittels 51 parallel zur Ausschubrichtung 16 und zum Verlauf des Führungskanals 37 des mechanischen Schlüsselteils 35 verläuft. In der Seitenwand 43 des Führungskanals 37 ist eine längliche Öffnung 44 vorgesehen, durch die das Stellglied 47 hindurchgreift. Das Zugmittel 51 ist auf der dem Führungskanal 37 abgewandten Seite des Stellgliedes 47 mit dessen Nase 48 verbunden.

In der Ruhestellung 11 des mechanischen Schlüsselteils 35 befindet sich die Nase 48 des Stellgliedes 47 an dem, die Längsöffnung 44 im rückwärtigen Bereich begrenzenden Anschlag 54. Der Schlüssel ist in der Ruhestellung 11 gänzlich in das Gehäuseteil 30 eingefahren. Zur Überführung des mechanischen Schlüsselteils 35 in



seiner Arbeitsstellung 15 muss nun die Auslösetaste 70 und somit der Hebel 71 betätigt werden, so dass der Rasthaken 72 aus der Aussparung 75 im mechanischen Schlüsselteil 35 herausfährt. Das mechanische Schlüsselteil 35 verfährt nun unter Einwirkung des Zugkraftspeichers 50 in Ausschubrichtung 16 aus dem Gehäuseteil 30 hinaus in seine Arbeitsstellung 15. Bei Erreichen der Arbeitsstellung 15 fährt die Nase 48 des Stellgliedes 47 gegen den Anschlag 49, der die Öffnung 44 an ihrem der Schlüsselöffnung zugewandten Ende begrenzt. Sobald das mechanische Schlüsselteil 35 in dieser Stellung ist, rastet zusätzlich noch der Rasthaken 74 in der Aussparung 75 am mechanischen Schlüsselteil 35 unter der Kraft der Feder 77 ein.

Zum Rücküberführen des mechanischen Schlüsselteiles 35 aus seiner Arbeitsstellung 15 in die Ruhestellung 11 muss wiederum die Auslösetaste 70 manuell betätigt werden, wodurch der Hebel 73 verschwenkt wird und der daran angeordnete Rasthaken 74 aus der Aussparung 75 im mechanischen Schlüsselteil 35 herausfährt. Hierdurch kann nun das mechanische Schlüsselteil 35 manuell wieder in den Führungskanal 37 im Gehäuseteil 30 eingeschoben werden. Kurz vor Erreichen der Ruhestellung 11 fährt das mechanische Schlüsselteil 35 mit seinem hinteren Ende im Bereich seiner Auflaufschräge 85 gegen den Rasthaken 72 und stößt diesen gegen die Kraft der Feder 77 aus dem Führungskanal 37 hinaus. Der Rasthaken 72 schnappt dann bei Erreichen der Ruhestellung 11 durch das mechanische Schlüsselteil wieder in die Aussparung 75 ein und verrastet dort das mechanische Schlüsselteil 35.

Durch die manuelle Rücküberführung des mechanischen Schlüsselteils 35 in die Ruhestellung 11 ist der Zugkraftspeicher 50 wieder vorgespannt worden, so dass er bei einer erneuten Betätigung der Auslösetaste 70 das mechanische Schlüsselteil 35 wiederum aus seiner Ruhestellung 11 in seine Arbeitsstellung 15 überführen kann.

In den Fig. 9 und 10 ist nun ein weiteres Ausführungsbeispiel des erfindungsgemäßen Schlüssels dargestellt. In einem Gehäuseteil 30' ist wiederum ein mechanisches Schlüsselteil 35' in einem in dem Gehäuseteil 30' liegenden Führungskanal 37' verschieblich angeordnet. Der Führungskanal 37' wird gebildet aus den beiden Flächenwänden 40' und 41', die Abschnitten der Flächenseiten 38' und 39' der Gehäusegrundplatte 32' und des Gehäusedeckels 31' entsprechen. Die Seiten des Führungskanals 37' werden durch Wände 42' und 43' gebildet. In der Wand 43' ist eine Öffnung 44' vorgesehen, durch die ein als Zahnrad ausgeformtes Stellglied 47' hindurchgreift und die Zähne 62 des Zahnrades 47' in eine Zahnung 64 am mechanischen Schlüsselteil 35' eingreifen. Das Zahnrad 47' sitzt auf einer Achse 63, die in diesem Ausführungsbeispiel an der Gehäusegrundplatte 32' angeformt ist. Das Zahnrad 47' weist in seinem oberen Bereich einen Hohlraum auf, in dem ein Druckkraftspeicher 60, wie eine Spiralfeder angeordnet ist. Im unteren Umfangsbereich des Zahnrades unterhalb der Zahnung 62 ist eine Aussparung 76 vorgesehen, in die der Rasthaken 72' eines Hebels 71' hineinragt, wenn das mechanische Schlüsselteil 35' sich in seiner Ruhestellung oder seiner Arbeitsstellung befindet. Wie schon im vorausgehenden Ausführungsbeispiel ist der Hebel 71' über eine Auslösetaste 70' zu betätigen. Der Rasthaken steht wiederum unter der Kraft der Feder 77', die zwischen der rahmenseitigen Federsitz 78' und der Ansatzstelle 79' am Hebel 70' angeordnet ist. In Fig. 9 ist das mechanische Schlüsselteil 35' in seiner Arbeitsstellung 15 dargestellt. Strichpunktiert dargestellt ist ferner noch die Ruhestellung des mechanischen Schlüsselteils 35'.

An dem gehäuseteilseitigen Ende des mechanischen Schlüsselteils 35' ist eine Nase 48' in Richtung der Wand 42' an dem mechanischen Schlüsselteil 35' angeformt. Diese Nase 48' ist in einer Öffnung 46', die in der Wand 42' parallel zum Führungskanal 37' und der Ausschubrichtung 16 des mechanischen Schlüsselteils 35' verläuft, angeordnet. Durch die Nase 48' wird die Ausschubbewegung des mechanischen Schlüsselteils 35', die durch den Druckkraftspeicher 60 mittels des Zahnrades 47' auf das mechanische Schlüsselteil 35' übertragen wird, wenn die

Auslösetaste 70' gedrückt worden ist, begrenzt, da die Nase 48' beim Erreichen der Arbeitsstellung 15 gegen den Anschlag 49' fährt.

Zum Einfahren des mechanischen Schlüsselteils 35' muss wiederum die Auslösetaste 70' betätigt werden, so dass der Rasthaken 72' aus der Aussparung 76 herausfährt und derart eine Drehbewegung des Zahnrades 47' ermöglicht wird. Das mechanische Schlüsselteil 35' kann nun wieder in den Führungskanal 37' des Gehäuseteils 30' eingeschoben werden, wobei das Zahnrad 47' mitgedreht wird und derart der Druckkraftspeicher 60 bzw. die Spiralfeder wieder aufgezogen wird, um ein erneutes Ausfahren zu erlauben. Der Einschiebevorgang wird beendet, wenn die Nase 48' vor den Anschlag 54' läuft, der die Öffnung 46' an ihrem rückwärtigen Ende begrenzt. In der nun erreichten Ruhestellung 11 schnappt der Rasthaken 72' wieder in die Aussparung 76 am unteren Rand des Zahnrads 47' ein. Das mechanische Schlüsselteil 35' ist nunmehr in der Ruhestellung 11 verrastet. Das Verrasten des Rasthakens 72' in die Aussparung 76 am unteren Rand des Zahnrades 47' erfolgt also bei ein- und ausgeschobenem mechanischen Schlüsselteil. Dies bedeutet, dass eine Umdrehung des Zahnrades 47' gleich dem Hub des mechanischen Schlüsselteils sein muss.

Ein erneutes Ausfahren in die Arbeitsstellung 15 kann wiederum durch Betätigen der Auslösetaste 70' erfolgen, wodurch der Rasthaken 72' erneut aus der Aussparung 76 ausfährt und das Zahnrad 47', welches nunmehr freigegeben ist mit der Kraft der Spiralfeder 60 das mechanische Schlüsselteil 35' aus dem Führungskanal 37' hinausfährt und in die Arbeitsstellung 15 überführt.

In den Fig. 11 und 12 ist nun ein drittes Ausführungsbeispiel des erfindungsgemäßen Schlüssels wiedergegeben. Das mechanische Schlüsselteil 35'' ist in einem Gehäuseteil 30'' in einem Führungskanal 37'' angeordnet. Die Flächenwände 40'' des Führungskanals 37'' werden wiederum gebildet aus den Flächenseiten 38'' der Gehäusegrundplatte 32'' und der nicht dargestellten

Flächenseite des ebenfalls nicht dargestellten Gehäusedeckels. An den Schmalseiten des Führungskanals sind Wände 42'' und 43'' angeordnet, die bei diesem Ausführungsbeispiel jeweils einen Kanal 67 und einen Kanal 68 aufweisen. Die Wand 43'' weist eine längliche Öffnung 44'' auf, die parallel zur Ausschubrichtung 16 des mechanischen Schlüsselteils 35'' verläuft. Im hinteren Bereich des Gehäuseteils 30'' ist ein Druckkraftspeicher 60'' wie eine Spiralfeder angeordnet, die auf ein Zahnrad 65 einwirkt, welches drehbar auf einer Achse 63'' gelagert ist. Die Zahnung 62'' am Zahnrad 65 greift in Zahnöffnungen 66 eines Schubmittels 61, wie etwa eines Zahnriemens ein, der in den Kanälen 67 und 68, sowie um das Zahnrad 65 herum und an dem dort gegenüberliegenden Wandabschnitt 53'' geführt ist. Am vorderen Ende dieses Schubmittels/Zahnriemens 61 ist ein Stellglied 47'' angeordnet, mittels dessen eine vom Zahnriemen 61 ausgeübte Stellbewegung auf das mechanische Schlüsselteil 35'' übertragen werden kann. Am vorderen Ende des Zahnriemens 61 ist ebenfalls ein Sperrmittel 76' angeordnet, welches in der Ruhestellung 11 des mechanischen Schlüsselteils 35'' an dem Rasthaken 72'' eines Hebels 71'' unter der Stellkraft des Druckkraftspeichers 60'' anliegt. Das Sperrmittel 76' liegt dabei über dem Wandabschnitt 53'' der Wand 47''.

Der Hebel 71'' ist auf einer Achse 81'' verschwenkbar gelagert. Er weist an seinem zweiten Ende eine Auslösetaste 70'' auf, mittels derer der Rasthaken 72'' entgegen der Federkraft einer Feder 77'', die an den Ansatzstellen 79'' und 78'' zwischen dem vorderen Arm des Hebels 71'' und der gehäuseseitigen Wand 43'' angeordnet ist.

In Fig. 11 ist der erfindungsgemäße Schlüssel in der Ruhestellung 11 des mechanischen Schlüsselteils 35'' dargestellt. Das mechanische Schlüsselteil 35'' liegt dabei gänzlich in dem Führungskanal 37'' gehäuseseitig hinter der Schlüsselstellung 12.

Wird die Auslösetaste 70'' betätigt, und der Hebel 71'' entgegen der Kraft der Feder 77'' verschwenkt, so gibt der Rasthaken 72'' das Sperrmittel/Sperrglied 76' frei. Hierdurch kann nun das Schubmittel 61 mit dem daran angeordneten Stellglied 47'' aufgrund des von dem Druckkraftspeicher 60'' ausgeübten Bewegungsmomentes das von dem Druckkraftspeicher 60'' auf das Zahnrad 65 und von diesem über die Zahnung 62'' und die Zahnöffnung 66 auf das Schubmittel 61 übertragen wird in Ausschubrichtung 16 auf die Schlüsselöffnung 12 zubewegt, wodurch der über das Stellglied 47'' betätigte mechanische Schlüsselteil 35'' aus dem Gehäuseteil 30'' heraus in seine Arbeitsstellung 15 verfahren wird. Beim Erreichen der Arbeitsstellung 15 fährt die Nase 48'' des Stellgliedes 47'' vor einem Anschlag 49'', der am Ende der Öffnung 44'' angeordnet ist. Ein Sperrmittel 76'', welches in Ausschubrichtung mit einer Auflaufschräge versehen ist, ist bei der Ausschubbewegung hinter den Rasthaken 72'' gefahren, und verhindert nun über das Schubmittel 61 und das Stellglied 47'' ein Wiederhereinfahren des mechanischen Schlüsselteils 35''.

Bei erneuter Betätigung der Auslösetaste 70'' wird das Sperrmittel 76'' wieder freigegeben und es kann das mechanische Schlüsselteil 35'' wieder manuell in den Führungskanal 37'' im Gehäuseteil 30'' hineingeschoben werden. Hierdurch bewegt sich das Schubmittel 61 in reverser Richtung am Zahnrad 65 vorbei, welches hierdurch wieder bewegt wird, so dass die an dem Zahnrad 65 angelenkte und in dem Zahnrad 65 befindliche Spiralfeder 60'' mit der Einschubbewegung des mechanischen Schlüsselteils 35'' wieder gespannt wird. Kurz vor Erreichen der Ruhestellung 11 durch das mechanische Schlüsselteil 35'' fährt das Sperrmittel/Sperrglied 76' mit seiner Auflaufschräge gegen den Rasthaken 72'' und schiebt sich an diesem vorbei. Der Rasthaken 72'' fährt unter der Krafteinwirkung der Feder 77'' wieder hinter das Sperrmittel/Sperrglied 76' und blockiert ein Wiederherausfahren des mechanischen Schlüsselteils 35'' unter der Krafteinwirkung des Druckkraftspeichers/Spiralfeder 60''. Um ein zu weites Einschieben des mechanischen Schlüsselteils 35'' zu vermeiden, ist am hinteren Ende der Öffnung

44'' ein Anschlag 54'' vorgesehen, gegen den die Nase 48'' des Stellgliedes 47'' beim Einschieben des mechanischen Schlüsselteiles 35'' fährt. Gleichzeitig läuft das Sperrmittel 76'' gegen einen Anschlag 56, der am Ende der Wand 42'' liegt.

Neben den hier dargestellten Ausführungsbeispielen sind noch weitere Ausführungsformen denkbar. So sind insbesondere Ausführungsformen denkbar, bei denen die Schlüsselöffnung durch ein weiteres Mittel verschließbar ist, wenn das mechanische Schlüsselteil sich gänzlich im Führungskanal befindet.

Weiterhin ist z.B. eine Ausführungsform denkbar, bei der eine linear wirkende und linear verstellbare Druckfeder direkt auf ein Stellglied, wie z.B. das Stellglied 47 oder 47'' wirkt und derart ein mechanischer Schlüsselteil aus einem Gehäuseteil herausgeschoben werden kann. Eine solche linear wirkende Druckfeder kann z.B. in einem weiteren Führungskanal benachbart zum Führungskanal für das mechanische Schlüsselteil angeordnet sein, oder aber eine derartige Steifigkeit aufweisen, dass eine Führung des Federelementes nicht notwendig ist.

Ebenso könnte das mechanische Schlüsselteil über elektrisch angesteuerte solenoide oder durch hydraulisch wirkende Druckkraftspeicher aus dem Gehäuseteil ausgeschoben werden. Ebenso können anstelle einer Verrastung auch reibschlüssige Bremsmittel vorgesehen sein, die das mechanische Schlüsselteil jeweils in seinen Stellungen hält.

Es versteht sich ebenfalls, dass die Verbindungsmittel zwischen dem elektrischen Gehäuseteil und dem mechanischen Gehäuseteil auch anders als bei dem ersten Ausführungsbeispiel angeordnet sein können. So konnten die Nuten 27 und die Verrastmittelvorsprünge 28 auch in den Gehäusegrundplatten 32, 32', 32'' der die Schlüsselmechanik enthaltenden zweiten Gehäuseteile angeordnet sein. Die Schwalbenschwanzzapfen 23

müssten dann in den Gehäusegrundplatten 22 der, die Elektronik enthaltenden ersten Gehäuseteile angeordnet sein.

## Bezugszeichenliste:

- 10 Schlüssel
- 11 Ruhestellung
- 12 Schlüsselöffnung
  
- 14 Ebene
- 15 Arbeitsstellung
- 16 Ausschieberichtung / Ausfuhrichtung
- 17 Demontagerichtung
- 18 Montagerichtung
- 19 Öse
- 20 erstes Gehäuseteil mit  
Schlüsselektronik
- 21 Gehäusedeckel erstes Gehäuseteil
- 22 Gehäusegrundplatte erstes Gehäuseteil
- 23 Batteriefachdeckel
- 24 Batterie
- 25 Elektronikbauteile
- 26 Tastfelder
- 27 Nut in der Gehäusegrundplatte
- 28 Verrastmittelvorsprung
- 29 Schraubmittel
- 30 zweites Gehäuseteil mit  
Schlüsselmechanik
- 30' zweites Gehäuseteil mit  
Schlüsselmechanik
- 30'' zweites Gehäuseteil mit  
Schlüsselmechanik
- 31 Gehäusedeckel zweites Gehäuseteil



- 31' Gehäusedeckel zweites Gehäuseteil
- 32 Gehäusegrundplatte
- 32' Gehäusegrundplatte
- 32'' Gehäusegrundplatte
- 33 Schwalbenschwanzzapfen
- 34 Frontteil der Gehäusegrundplatte
- 35 Schlüsselteil
- 35' Schlüsselteil
- 36 Gehäuseinnenraum (zweites Gehäuseteil)
- 37 Führungskanal
- 37' Führungskanal
- 37'' Führungskanal
- 38 Flächenseite
- 38' Flächenseite
- 38'' Flächenseite
- 39 Flächenseite
- 39' Flächenseite
- 40 Flächenwand
- 40' Flächenwand
- 40'' Flächenwand
- 41 Flächenwand
- 41' Flächenwand
- 42 Wand
- 42' Wand
- 42'' Wand
- 43 Wand
- 43' Wand
- 43'' Wand
- 44 Längsöffnung
- 44' Öffnung

- 44'' Längsöffnung
- 45 Öffnung
- 46 Öffnung
- 46' Öffnung
- 47 Stellglied
- 47' Stellglied / Zahnrad
- 47'' Stellglied
- 48 Nase
- 48' Nase
- 48'' Nase
- 49 Anschlag (Arbeitsstellung)
- 49' Anschlag (Arbeitsstellung)
- 49'' Anschlag (Arbeitsstellung)
- 50 Zugkraftspeicher
- 51 Zugmittel
- 52 Umlenkteil
- 53 Führungswand
- 53'' Wandabschnitt
- 54 Anschlag (Ruhestellung)
- 54' Anschlag (Ruhestellung)
- 54'' Anschlag (Ruhestellung)
- 55 Anschlag für Sperrmittel 76'
- 56 Anschlag für Sperrmittel 76''
- 60 Druckkraftspeicher
- 60'' Druckkraftspeicher
- 61 Schubmittel
- 62 Zähne am Stellglied 47'
- 62'' Zähne am Zahnrad 65
- 63 Achse
- 63'' Achse

- 64 Zahnung am Schlüssel 35' /Schubmittel
- 65 Zahnrad / Schubmittel
- 66 Zahnöffnung / Schubmittel 61
- 67 Kanal
- 68 Kanal
- 70 Auslösetaste (Auslösemittel)
- 70' Auslösetaste (Auslösemittel)
- 70'' Auslösetaste (Auslösemittel)
- 71 Hebel
- 71' Hebel
- 71'' Hebel
- 72 Rasthaken von Hebel 71
- 72' Rasthaken von Hebel 71
- 72'' Rasthaken von Hebel 71
- 73 Hebel
- 74 Rasthaken von Hebel 73
- 75 Sperrmittel / Aussparung
- 75'' Sperrmittel
- 76 Sperrmittel / Aussparung
- 76' Sperrmittel
- 76'' Sperrmittel
- 77 Druckmittel / Feder
- 77' Druckmittel / Feder
- 77'' Druckmittel / Feder
- 77''' Druckmittel / Feder
- 78 Federsitz
- 78' Federsitz
- 78'' Federsitz
- 78''' Federsitz
- 79 Ansatzstelle

79' Ansatzstelle

79'' Ansatzstelle

79''' Ansatzstelle

81 Hebelachse

81' Hebelachse

81'' Hebelachse

83 Hebelachse

84 Berührungsstelle

85 Auflaufschräge

## P a t e n t a n s p r ü c h e :

1. Schlüssel, insbesondere für Kfz, mit einem Gehäuseteil (30, 30', 30'') und einem daran angeordneten mechanischen Schlüsselteil (35, 35', 35''),

bei dem wenigstens ein schließwirksamer Teil des Schlüsselteils (35, 35', 35'') mittels einer Mimik (47-47'', 50, 51, 52, 60, 60'', 61, 62, 62'', 64, 65, 66) von einer Ruhestellung (11) in eine Arbeitsstellung (15) zu überführen ist, in der der Schlüssel (10) zur mechanischen Betätigung eines Schlosses benutzt werden kann,

wobei zur Aktivierung der Mimik (47-47'', 50, 51, 52, 60, 60'', 61, 62, 62'', 64, 65, 66) ein manuell zu betätigendes Auslösemittel (70) vorgesehen ist,

und das Schlüsselteil (35, 35', 35'') in der Arbeitsstellung (15) im wesentlichen bewegungsstarr ist,

dass das Schlüsselteil (35, 35', 35'') in seiner Ruhestellung (11) in einem Gehäuseinnenraum (36) angeordnet ist,

und dass das Schlüsselteil (35, 35', 35'') nach einer Betätigung des Auslösemittels (70) mittels der Mimik (47-47'', 50, 51, 52, 60, 60'', 61, 62, 62'', 64, 65, 66) von seiner Ruhestellung (11) im Gehäuseinnenraum (36) durch eine laterale Verschiebung aus dem Gehäuseteil (30, 30', 30'') heraus, in die Arbeitsstellung (15) zu überführen ist,

und in dem Gehäuseinnenraum (36) Mittel (37, 40, 41, 42, 43) angeordnet sind, durch die das Schlüsselteil (35, 35', 35'') bei der Längsverschiebung geführt ist,

dadurch gekennzeichnet,

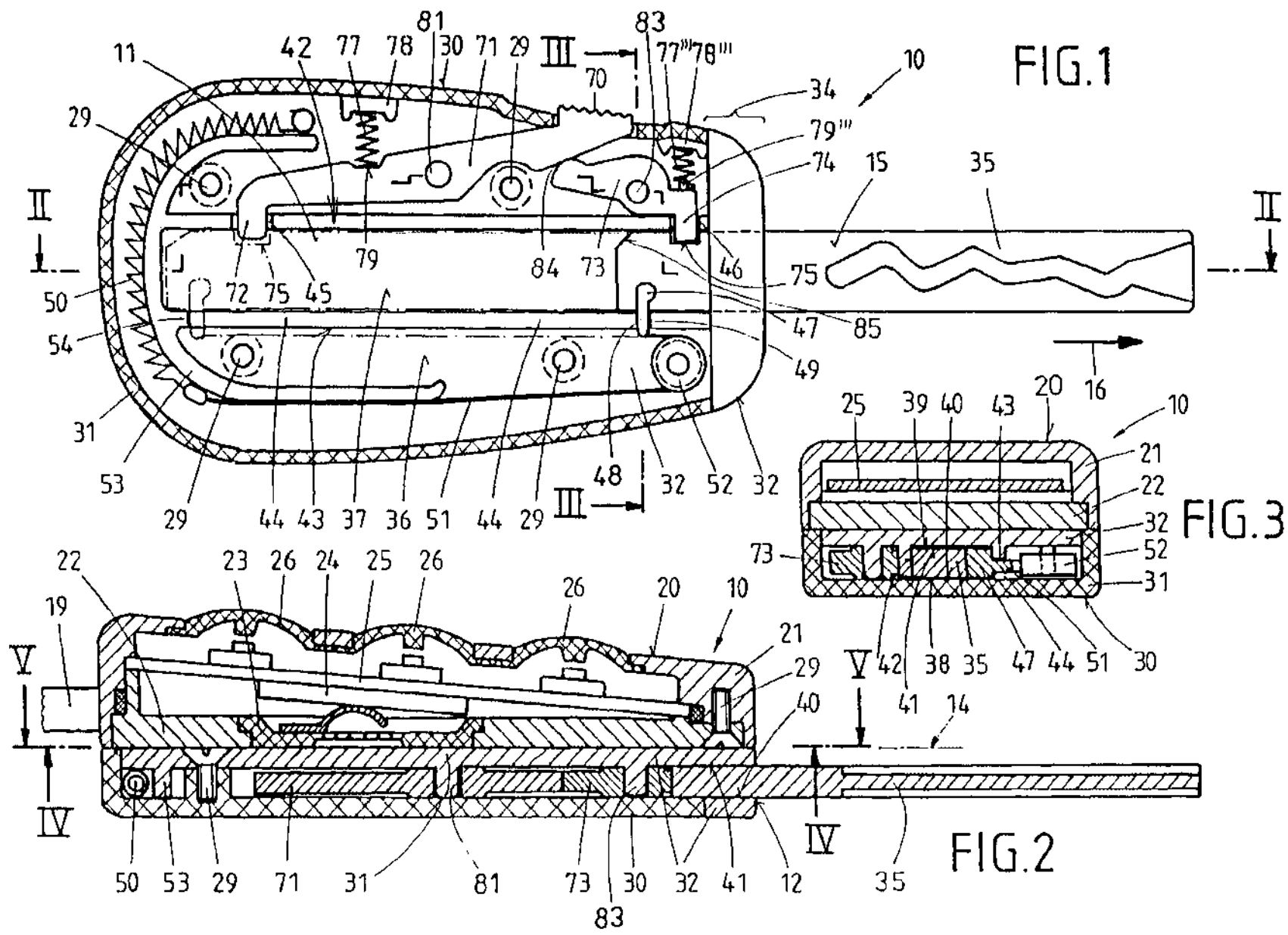
dass die Mimik (47-47'', 50, 51, 52, 60, 60'', 61, 62, 62'', 64, 65, 66) einen Zug- (50) oder Druckkraftspeicher (60) umfasst, der indirekt über ein Zug- (51) oder Schubmittel (61, 64, 65, 66) an dem Stellglied (47) angreift.

2. Schlüssel nach Anspruch 1, dadurch gekennzeichnet, dass in dem Gehäuseteil (30, 30', 30'') in Ausschubrichtung (16) des Schlüsselteils (35, 35', 35'') eine Schlüsselöffnung (12) angeordnet ist, die formschlüssig zur Außenkontur des Schlüsselteils (35, 35', 35'') ausgebildet ist.
3. Schlüssel nach einem der Ansprüche 1 oder 2, dadurch gekennzeichnet, dass der Gehäuseinnenraum (36) des Gehäuseteils (30, 30', 30'') über ein an der Schlüsselöffnung (12) angeordnetes Verschlussmittel von dem, das Gehäuseteil (30, 30', 30'') umgebenden Außenraum abgeschlossen ist.
4. Schlüssel nach Anspruch 1, dadurch gekennzeichnet, daß die Mittel zur Führung des Schlüsselteils (35, 35', 35'') einen Führungskanal (37) umfassen.
5. Schlüssel nach einem der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass das, den mechanischen Schlüsselteil (35, 35', 35'') und die Mimik (47 - 47'', 50, 51, 52, 60, 60'', 61, 62, 62'', 64, 65, 66) beherbergende Gehäuseteil (30, 30', 30'') wenigstens zwei, im wesentlichen parallel zueinander verlaufende Flächenseiten (38, 38', 39, 39'') aufweist, und diese Flächenseiten (38, 38', 39, 39'') zu zwei Seiten die Flächenwände (40, 40', 40'', 41, 41') des Führungskanals (37) bilden.

6. Schlüssel nach einem der Ansprüche 1 und 5, dadurch gekennzeichnet, dass im wesentlichen senkrecht zu den Flächenwänden (40, 40', 40'', 41, 41') zwei im wesentlichen parallel verlaufende Wände (42, 42', 42'', 43, 43', 43'') den Führungskanal (37) seitlich begrenzen.
7. Schlüssel nach einem der Ansprüche 1 und 6, dadurch gekennzeichnet, dass wenigstens eine Wand (42, 42', 42'', 43, 43', 43'') des Führungskanals eine Öffnung (44, 44', 44'') aufweist durch den ein, auf das mechanische Schlüsselteil (35, 35', 35'') einwirkendes Stellglied (47, 47', 47'') der Mimik die Wand (42, 42', 42'', 43, 43', 43'') durchgreift.
8. Schlüssel nach einem der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass die Öffnung (44, 44'') im wesentlichen linear und parallel zur Ausschiebrichtung (16) des mechanischen Schlüsselteils (35, 35', 35'') verläuft.
9. Schlüssel nach Anspruch 1, dadurch gekennzeichnet, dass ein Endanschlag (49, 49'') vorgesehen ist, gegen den eine am Schlüsselteil (35, 35', 35'') angeordnete Nase (48, 48', 48'') zur Begrenzung des Ausschubwegs aufläuft.
10. Schlüssel nach Anspruch 1, dadurch gekennzeichnet, dass der mechanische Schlüsselteil (35, 35', 35'') durch Rastmittel (71 - 71'', 72 - 72'', 73, 74, 75, 76-76'') in seiner Ruhe- (11) und in seiner Arbeitsstellung (15) bewegungsstarr gehalten ist.
11. Schlüssel nach einem der Ansprüche 1 und 10, dadurch gekennzeichnet, dass die Rastmittel (71 - 71'', 72 - 72'', 73, 74, 75, 76-76'') durch Betätigung des Auslösemittels (70 - 70'') freigegeben werden.

12. Schlüssel nach einem der Ansprüche 1 bis 11, dadurch gekennzeichnet, dass die Rastmittel wenigstens einen Hebel (71 - 71'', 73) mit wenigstens einem Rasthaken (72 - 72'', 74) umfassen, der in der Arbeits- (15) und/oder Ruhestellung (11) jeweils auf ein Sperrmittel (75 - 75'', 76, 76') einwirkt.
13. Schlüssel nach Anspruch 1, dadurch gekennzeichnet, dass der Zugkraftspeicher (50) über ein Zugmittel (51) an dem Stellglied (47) angreift, wobei der Zugweg des Zugmittels (51) und des Zugkraftspeichers (50) durch Umlenkung des Zugmittels (51) an einem Umlenkteil (52), insbesondere einer Umlenkrolle, vergrößert ist.
14. Schlüssel nach Anspruch 1, dadurch gekennzeichnet, dass der Druckkraftspeicher (60) über Schubmittel (61, 64, 65, 66) an dem Stellglied (47'') angreift.
15. Schlüssel, nach Anspruch 1, dadurch gekennzeichnet, dass zwei in sich abgeschlossene Gehäuseteile (20, 30; 20', 30'; 20'', 30'') aneinander angeordnet sind, wobei das erste Gehäuseteil (20, 20', 20'') eine Schlüsselektronik (25, 24), und das zweite Gehäuseteil (30; 30'; 30'') einen mechanischen Schlüsselteil (35, 35', 35'') und eine Mimik (47 - 47'', 50, 51, 52, 60, 60'', 61, 62, 62'', 64, 65, 66) beinhaltet, und bei dem die beiden Gehäuseteile (20, 30; 20', 30', 20'', 30'') entlang einer einzelnen, im wesentlichen planaren Ebene (14) reversibel aneinander festgelegt sind.
16. Schlüssel nach Anspruch 15, dadurch gekennzeichnet, dass im Bereich der planaren Ebene (14) Verbindungsmittel (28, 30) an den Gehäuseteilen 20, 30; 20', 30'; 20'', 30'') angeordnet sind, mittels derer die Gehäuseteile (20, 30; 20', 30'; 20'', 30'') reversibel aneinander festgelegt sind.





214

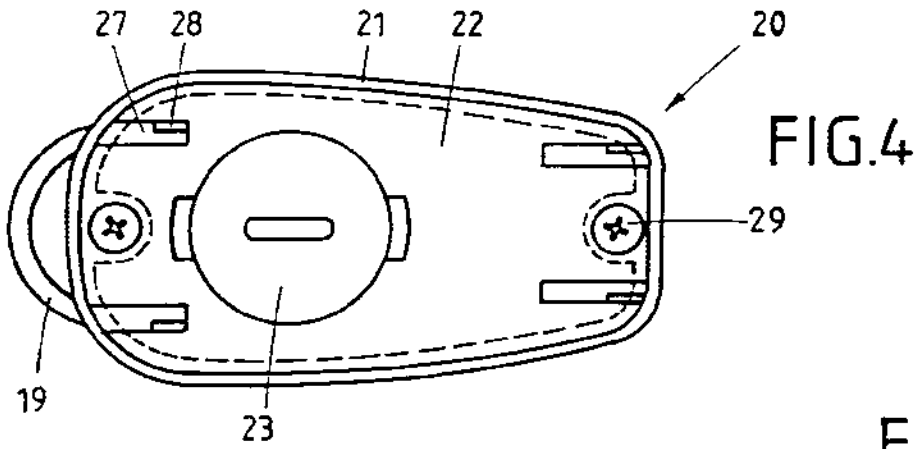


FIG. 4

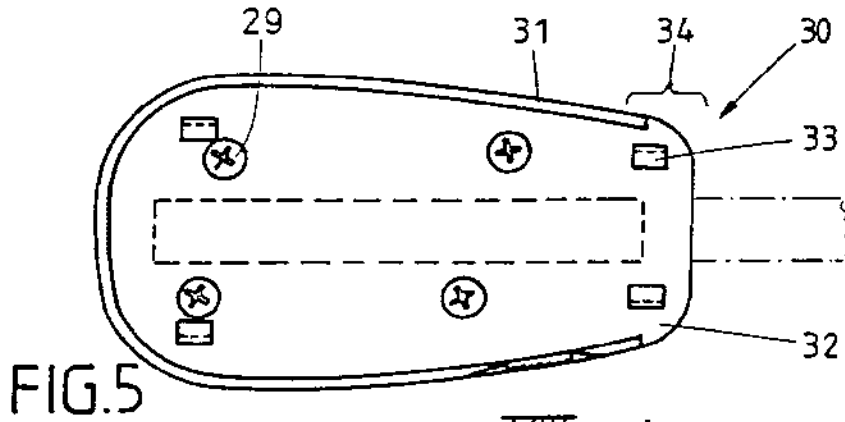


FIG. 5

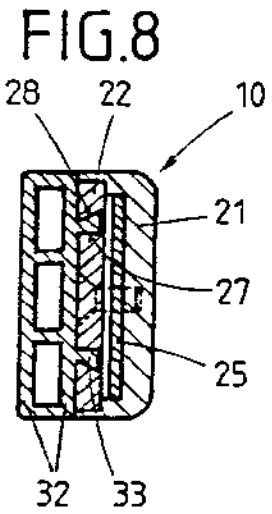


FIG. 8

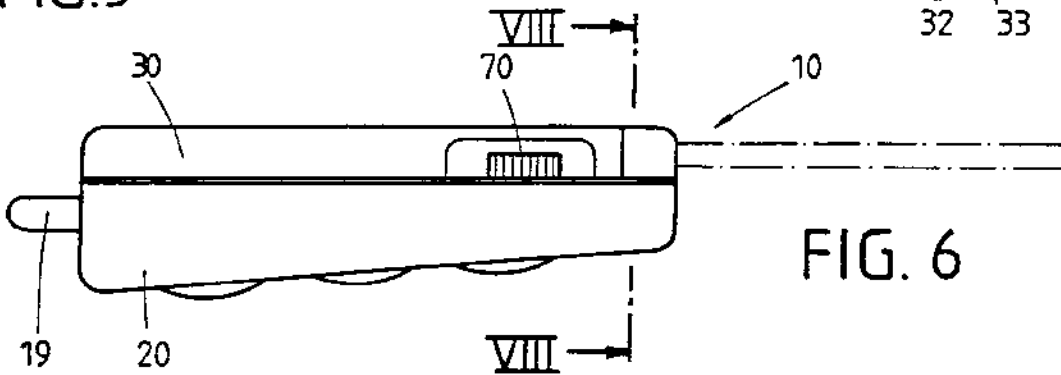


FIG. 6

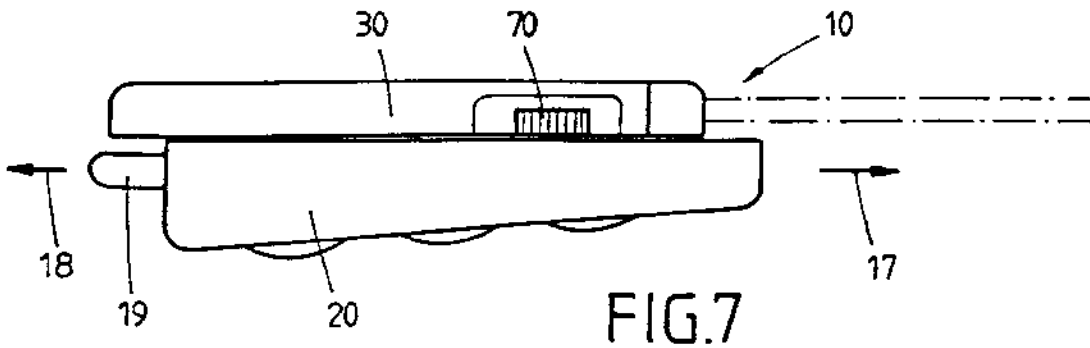


FIG. 7

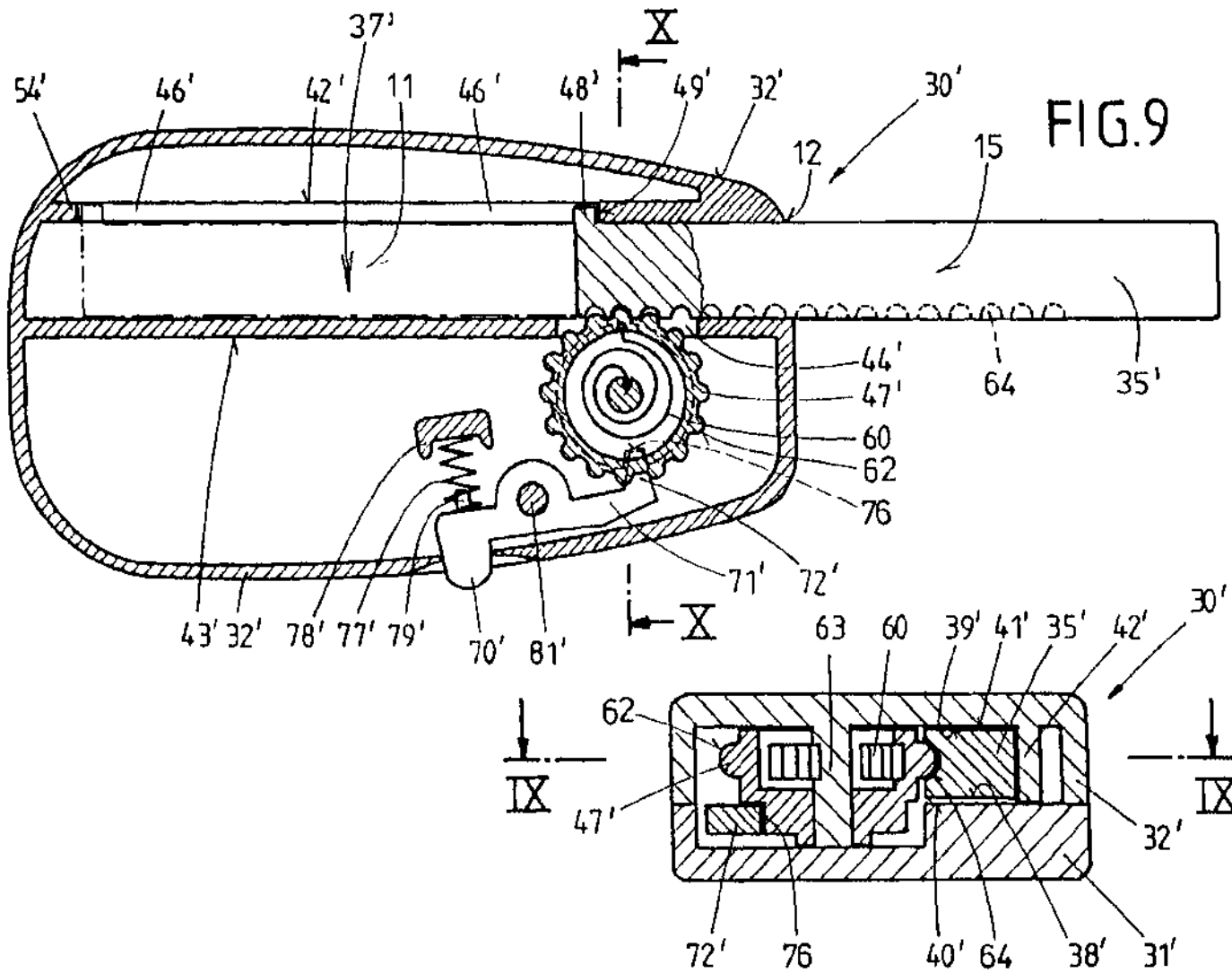
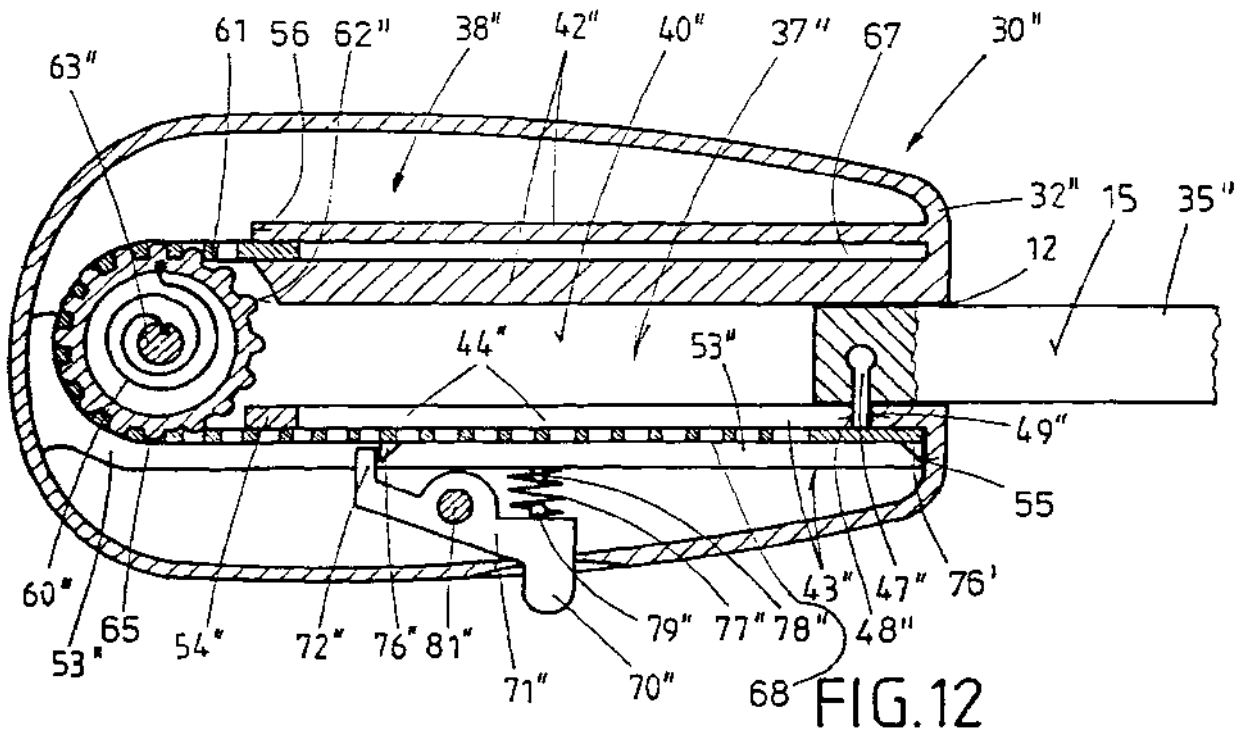
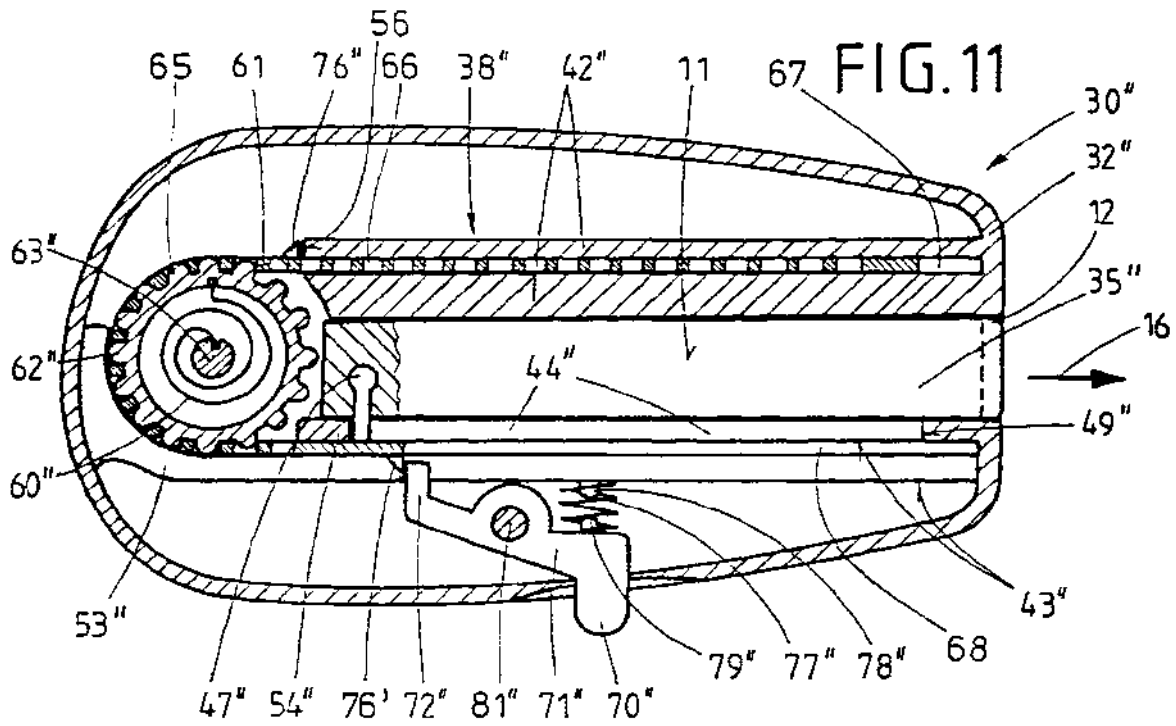


FIG. 10



# INTERNATIONAL SEARCH REPORT

International Application No

PCT/EP 00/11504

**A. CLASSIFICATION OF SUBJECT MATTER**  
 IPC 7 E05B19/04 A45C11/32

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 A45C 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)

EPO-Internal

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P,X	DE 199 12 749 C (VALEO GMBH & CO SCHLIESSYST KG) 2 November 2000 (2000-11-02) column 3, line 35 - line 59; figure	1-5, 7-12, 14-16
X	US 2 690 666 A (MORRIS ENGEL ET AL.) 5 October 1954 (1954-10-05) cited in the application column 4, line 7 - line 51; figure	1, 2, 4-6, 9-12
X	US 3 328 986 A (THEODORE RALTON) 4 July 1967 (1967-07-04) column 2, line 35 - line 62; figure	1, 2, 4-6, 9-11, 14
A	FR 2 597 537 A (PEUGEOT) 23 October 1987 (1987-10-23) page 3, line 4 - line 24; figures 1,3,4	15

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

10 April 2001

Date of mailing of the international search report

20/04/2001

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

Pieracci, A

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 00/11504

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 19912749 C	02-11-2000	NONE	
US 2690666 A	05-10-1954	NONE	
US 3328986 A	04-07-1967	NONE	
FR 2597537 A	23-10-1987	NONE	

# INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP 00/11504

**A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES**  
 IPK 7 C05B19/04 A45C11/32

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

**B. RECHERCHIERTE GEBIETE**

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)  
 IPK 7 A45C 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)

EPO-Internal

**C. ALS WESENTLICH ANGESEHENE UNTERLAGEN**

Kategorie	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruchs Nr.
P, X	DE 199 12 749 C (VALEO GMBH & CO SCHLIESSYST KG) 2. November 2000 (2000-11-02) Spalte 3, Zeile 35 - Zeile 59; Abbildung	1-5, 7-12, 14-16
X	US 2 690 666 A (MORRIS ENGEL ET AL.) 5. Oktober 1954 (1954-10-05) in der Anmeldung erwähnt Spalte 4, Zeile 7 - Zeile 51; Abbildung	1, 2, 4-6, 9-12
X	US 3 328 986 A (THEODORE RALTON) 4. Juli 1967 (1967-07-04) Spalte 2, Zeile 35 - Zeile 62; Abbildung	1, 2, 4-6, 9-11, 14
A	FR 2 597 537 A (PEUGEOT) 23. Oktober 1987 (1987-10-23) Seite 3, Zeile 4 - Zeile 24; Abbildungen 1, 3, 4	15

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 worden 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 erfinderscher Tätigkeit beruhend betrachtet werden
- \*Y\* Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderscher 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
- \*Z\* Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche: 10. April 2001  
 Abschlusssdatum des internationalen Recherchenberichts: 20/04/2001

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: Pieracci, A

# INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Abzeichen

PCT/EP 00/11504

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 19912749 C	02-11-2000	KEINE	
US 2690666 A	05-10-1954	KEINE	
US 3328986 A	04-07-1967	KEINE	
FR 2597537 A	23-10-1987	KEINE	



(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
31 May 2001 (31.05.2001)

PCT

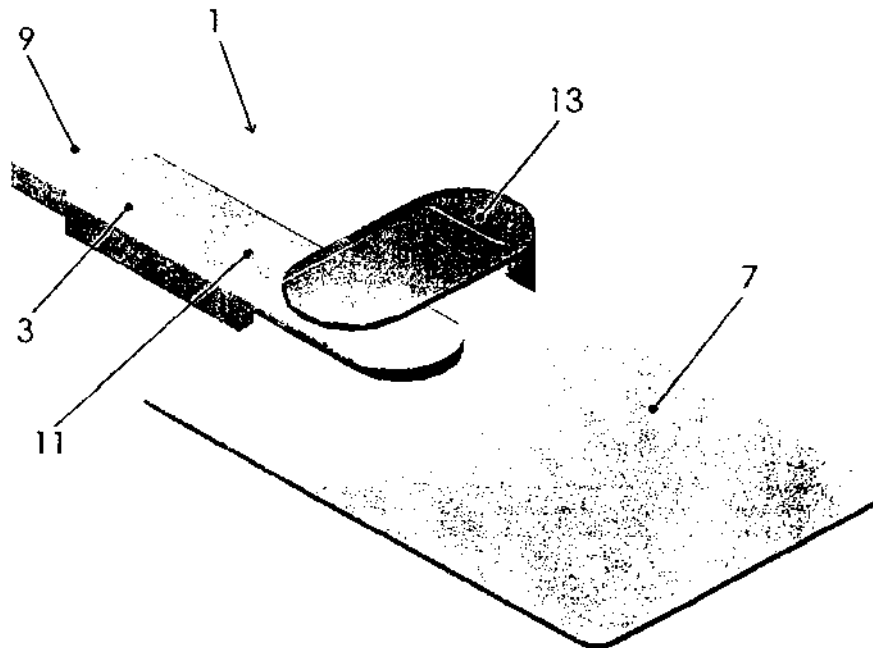
(10) International Publication Number  
**WO 01/39102 A1**

- (51) International Patent Classification<sup>7</sup>: G06K 7/00
- (21) International Application Number: PCT/IT00/00429
- (22) International Filing Date: 25 October 2000 (25.10.2000)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:  
TO99A001020 22 November 1999 (22.11.1999) IT
- (71) Applicant (for all designated States except US): EUTRON INFOSECURITY S.R.L. [IT/IT]; Via Gandhi, 12, I-24048 Curnasco di Treviso (IT).
- (72) Inventors; and
- (75) Inventors/Applicants (for US only): CASSIA, Lucio [IT/IT]; c/o Eutron Infosecurity S.R.L., Via Gandhi, 12, I-24048 Curnasco di Treviso (IT). LEIDI, Michele [IT/IT]; c/o Eutron Infosecurity S.R.L., Via Gandhi, 12, I-24048 Curnasco di Treviso (IT).
- (74) Agent: GARAVELLI, Paolo; c/o A.Bre.Mar. S.r.l., Via Servais, 27, I-10146 Torino (IT).
- (81) Designated States (national): AE, AL, AU, BA, BB, BG, BR, CA, CN, CR, CU, CZ, DM, EE, GD, GE, HR, HU, ID, IL, IN, IS, JP, KP, KR, LC, LK, LR, LT, LV, MA, MG, MK, MN, MX, NO, NZ, PL, RO, SG, SI, SK, TR, TT, UA, US, UZ, VN, YU, ZA.
- (84) Designated States (regional): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW). Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM). European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE). OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

**Published:**  
— With international search report.

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: PORTABLE READER FOR SMART CARDS



(57) Abstract: 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).



WO 01/39102 A1

**PORTABLE READER FOR SMART CARDS**

The present invention refers to a portable reader for intelligent cards of the type commonly known as "smart cards".

Smart cards are nowadays rather widespread given their practical easiness of use: in fact, they allow, through microprocessors realised on integrated circuit chips obtained therein, to store a very high amount of data and therefore they can be used in applications such as different types of credit cards, cryptographic cards and future applications such as identity cards or electronic health cards.

For the purpose for which they are provided, such smart cards are adapted to communicate (that is, to transmit and receive) data through communication standards that are well-known at world level, such as the 7816 Standard. To realise such communication, the intelligent card is put in contact with a card reading device, which is equipped with suitable slots in which the card is

inserted, such slots containing a certain number of contacts that read the card data and communicate them to the microprocessor managing the card reader. Card readers are currently available on the market that are realised in the shape of boxes whose sizes are about 15 x 10 cm, that are statically connected to different types of data processing and transmitting systems. Such smart card readers are therefore with a relatively high encumbrance and due to their nature they are provided fixed in well-defined positions. On the market, there are currently no smart card readers that are portable and with small sizes.

Object of the present invention is solving the above prior-art problems, by providing a portable reader for smart cards that is of very reduced sizes and therefore can be easily transported and used by end users for any type of application.

A further object of the present invention is providing a portable reader that is equipped with such interface means as to allow it to widely and immediately use all smart cards with which a user can be equipped: for such purpose, the reader is equipped with means allowing it to be connected to a common Universal Serial Bus (USB) port of a

computer.

The above and other objects and advantages of the invention, as will appear from the following description, are obtained by a portable reader for smart cards as claimed in Claim 1. Preferred embodiments and non-trivial variations of the present invention are claimed in the dependent Claims.

The present invention will be better described by some preferred embodiments thereof, given as a non-limiting example, with reference to the enclosed drawings, in which:

- Figure 1 is a perspective view of an embodiment of a portable reader according to the present invention coupled with a smart card in the operating position;
- Figure 2 is a perspective view of the reader in Fig. 1 in the transport position;
- Figure 3 is a top view of the operating configuration in Fig. 1; and
- Figure 4 is a top view of the reader in Fig. 2.

With reference to the Figures, a preferred embodiment of the portable reader 1 for intelligent cards is shown, such cards being commonly known as

"smart cards".

The portable reader 1 for smart cards of the present invention substantially comprises a support body 3 shaped as an elongated box, comprising at one end thereof at least one slot 5 for inserting and reading therein a smart card 7. For such purpose, the slot 5 is equipped with reading means (not shown) for smart cards 7, that are commonly known and are composed of a plurality (usually six) of contacts that carry connection wires to a managing microprocessor (also not shown) contained inside the support body 3.

Such managing microprocessor is preferably realised through an integrated circuit chip and contains inside it all the necessary logics for receiving and transmitting data to the smart card 7 to which it is connected.

In order to communicate with the outside world the data obtained from a connected smart card 7, the portable reader 1 of the invention is further equipped with interface means 9 connected to the support body 3 and to the managing microprocessor; commonly, such interface means 9 are adapted to be connected to a common USB port of a computer, in order to be able to realise a connection with the

most widely known external managing networks (Internet, Intranet, etc.).

Moreover, the portable reader 1 of the invention comprises means 13 for keeping and aligning the smart card 7, that, in the practical embodiment shown, are composed of a bracket shaped as an elongated C and hinged to the support body 3 in order to have:

- a) an operating position in which the keeping and aligning means 13 are perpendicular to the support body 3 to keep the card 7 in contact with the reader 1 and to align the card 7 with the reading means (as can be clearly shown in Fig.s 1 and 3; and
- b) a rest position in which the keeping and aligning means 13 are aligned with the support body 3 allowing to transport and store the reader 1 (as can be clearly seen in Fig.s 2 and 4).

Finally, the portable reader 1 of the invention can be further equipped with means 11 that enable grasping the support body 3 by means of two fingers of an hand, such as for example the depression 11 shown in the different Figures.

A portable reader 1 has thereby been realised

that can be placed and stored in any suitable place and that can be easily transported and connected to USB ports: in this way, by arranging a reader whose overall sizes are on the order of 3 cm, it is possible to realise a flexible solution wherein each smart card with which a user is equipped can be immediately and easily connected and activated for the outside world to perform flexible and powerful applications.

Some preferred embodiments of the invention have been disclosed, but obviously they are subjected to further modifications and variations within the same inventive idea. For example, the reader 1 of the invention can be realised on a personal identification device like the one marketed by the Assignee of the present invention, containing in a single configuration the functionalities of personal identification, encrypted data transmission and smart cards reading. Otherwise, the reader 1 of the present invention can be pre-arranged in a stand-alone configuration according to application needs, guaranteeing at any rate an efficient solution as regards the practical comfort of the shape and portability of the reader 1 itself.

**CLAIMS**

1. Portable reader (1) for smart cards (7), characterised in that it comprises:
  - a support body (3) containing at least one slot (5) for inserting and reading a smart card (7), said slot (5) being equipped with reading means for smart cards (7);
  - interface means (9) connected to said support body (3);
  - means (13) for keeping and aligning said smart card (7); and
  - a managing microprocessor contained inside said support body (3) and connected to said interface means (9) and said reading means for smart cards (7).
2. Portable reader (1) according to Claim 1, characterised in that said interface means (9) are adapted to be connected to an USB port.
3. Portable reader (1) according to Claim 1, characterised in that said reading means for smart cards (7) are composed of a plurality of contacts carrying connection wires to said managing microprocessor.
4. Portable reader (1) according to Claim 3,



characterised in that said contacts are equal to six.

5. Portable reader (1) according to Claim 1, characterised in that said keeping and aligning means (13) are composed of an elongated-C-shaped bracket, said bracket being hinged to said support body (3) in order to have:
  - a. an operating position in which said keeping and aligning means (13) are perpendicular to said support body (3) to keep the card (7) in contact with said reader (1) and to align the card (7) with said reading means; and
  - b. a rest position in which said keeping and aligning means (13) are aligned with said support body (3) allowing to transport and store said reader (1).
6. Portable reader (1) according to Claim 1, characterised in that it is further equipped with means (11) that enable grasping said support body (3) by means of two fingers of an hand.

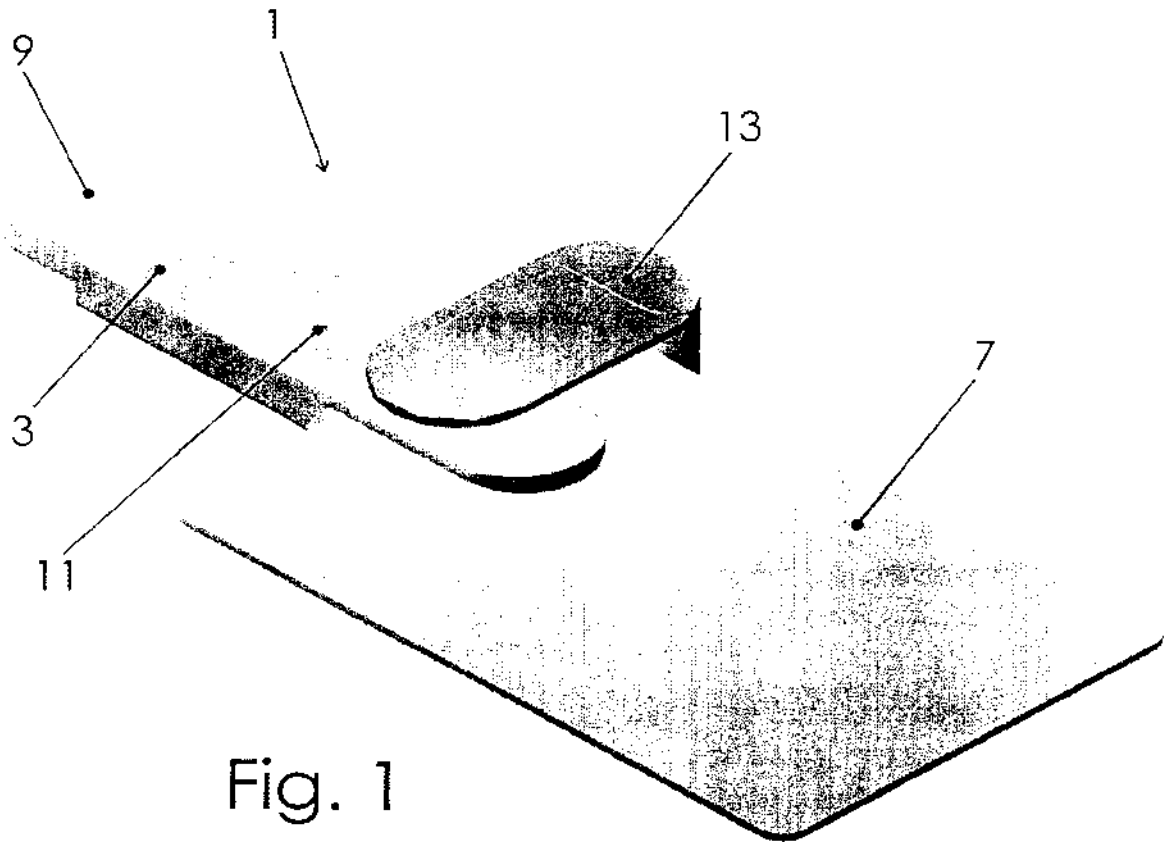


Fig. 1

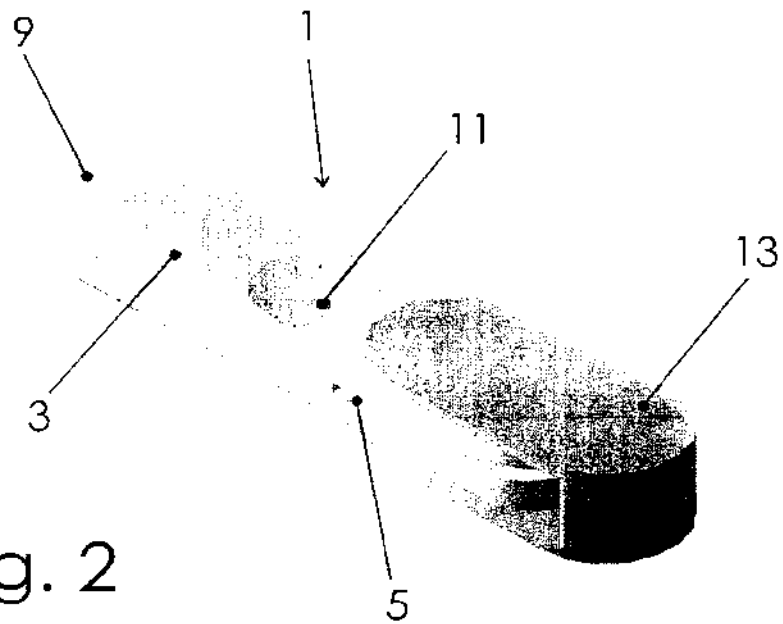


Fig. 2

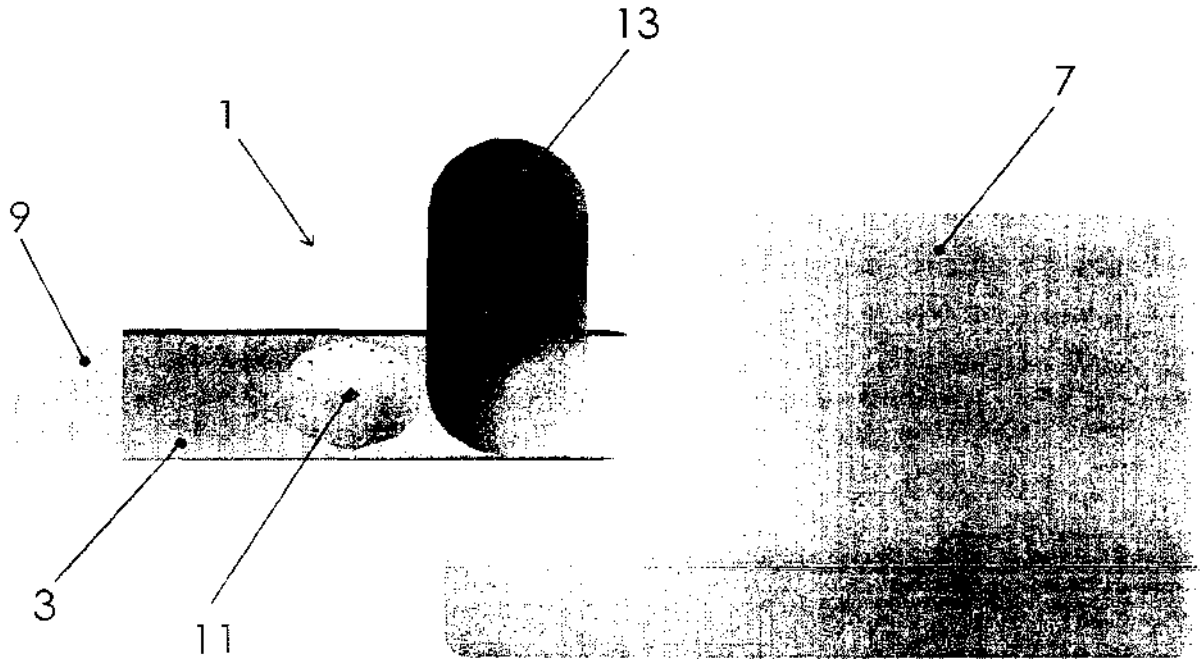


Fig. 3

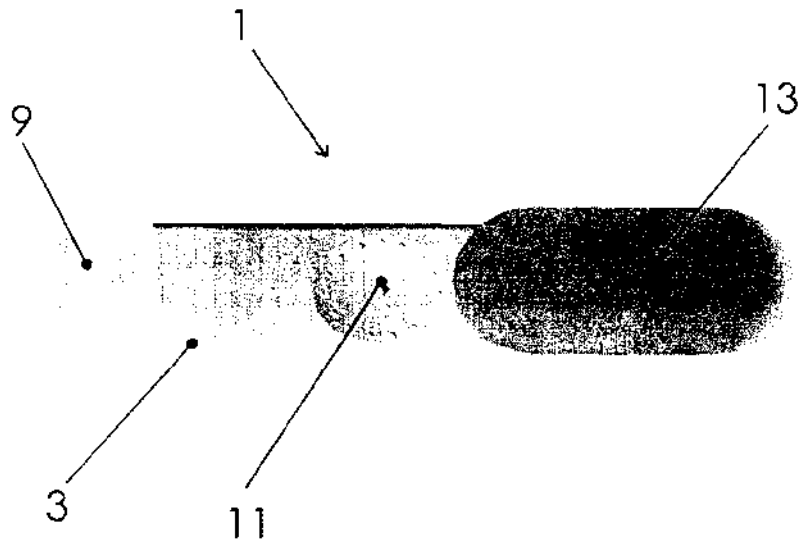


Fig. 4

# INTERNATIONAL SEARCH REPORT

International Application No

PCT/IT 00/00429

**A. CLASSIFICATION OF SUBJECT MATTER**  
IPC 7 G06K7/00

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 G06K G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data, PAJ

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category \* Citation of document, with indication, where appropriate, of the relevant passages

Relevant to claim No.

X	WO 97 07448 A (SIRBU CORNEL) 27 February 1997 (1997-02-27) page 9, line 14 -page 11, line 5 figures 1,7 ---	1-4,6
X	US 5 778 071 A (AMORUSO VICTOR P ET AL) 7 July 1998 (1998-07-07) column 2, line 24 - line 47 column 3, line 6 - line 8 column 6, line 62 -column 7, line 20 figure 1C ---	1,3,4,6
X	US 5 844 497 A (GRAY ROBERT J) 1 December 1998 (1998-12-01) column 3, line 36 -column 5, line 48 figures 1,2 --- -/--	1,3,4,6

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.
- \*Z\* document member of the same patent family

Date of the actual completion of the international search

Date of mailing of the international search report

30 January 2001

06/02/2001

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

Rydman, J

INTERNATIONAL SEARCH REPORT

International Application No

PCT/IT 00/00429

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 5 635 701 A (GLOTON JEAN-PIERRE) 3 June 1997 (1997-06-03) column 2, line 57 -column 3, line 13 figures 1,2 ---	1
A	FR 2 774 194 A (SCM SCHNEIDER MICROSYSTEME MIC) 30 July 1999 (1999-07-30) page 2, line 23 -page 3, line 30 figures 5,7 -----	1

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/IT 00/00429

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 9707448 A	27-02-1997	FR 2738070 A	28-02-1997
		FR 2740885 A	09-05-1997
		AU 720839 B	15-06-2000
		AU 6824096 A	12-03-1997
		BG 102336 A	30-12-1998
		BR 9610236 A	15-06-1999
		CN 1194043 A	23-09-1998
		CZ 9800408 A	16-12-1998
		EP 0870222 A	14-10-1998
		HU 9900499 A	28-06-1999
		JP 11511278 T	28-09-1999
		NO 980728 A	20-04-1998
		PL 325164 A	06-07-1998
		SK 22098 A	07-10-1998
US 6070796 A	06-06-2000		
US 5778071 A	07-07-1998	US 5546463 A	13-08-1996
		AU 726397 B	09-11-2000
		AU 4147097 A	06-03-1998
		EP 0916210 A	19-05-1999
		WO 9807255 A	19-02-1998
		US 5878142 A	02-03-1999
US 5844497 A	01-12-1998	US 6087955 A	11-07-2000
US 5635701 A	03-06-1997	FR 2716988 A	08-09-1995
		DE 69518678 D	12-10-2000
		EP 0670556 A	06-09-1995
		JP 7271888 A	20-10-1995
FR 2774194 A	30-07-1999	EP 1050006 A	08-11-2000
		WO 9938104 A	29-07-1999

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum  
Internationales Büro



(43) Internationales Veröffentlichungsdatum  
5. Juli 2001 (05.07.2001)

PCT

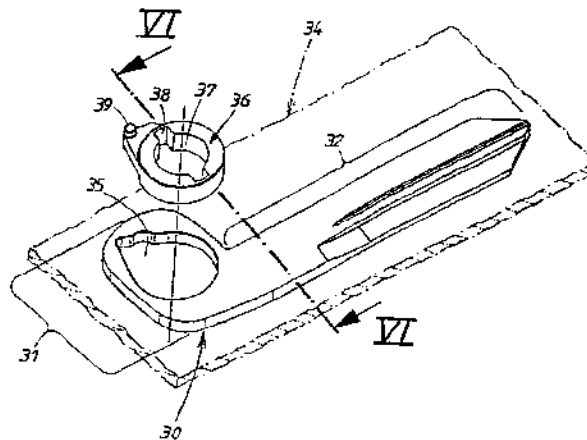
(10) Internationale Veröffentlichungsnummer  
WO 01/48339 A1

- (51) Internationale Patentklassifikation<sup>7</sup>: E05B 19/04, 49/00
- (21) Internationales Aktenzeichen: PCT/EP00/11619
- (22) Internationales Anmeldedatum:  
22. November 2000 (22.11.2000)
- (25) Einreichungssprache: Deutsch
- (26) Veröffentlichungssprache: Deutsch
- (30) Angaben zur Priorität:  
199 62 975.7 24. Dezember 1999 (24.12.1999) DE
- (71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von US): HUF HÜLSBECK & FÜRST GMBH & CO. KG [DE/DE]; Steeger Strasse 17, 42551 Velbert (DE).
- (72) Erfinder; und
- (75) Erfinder/Anmelder (nur für US): JACOB, Dirk [DE/DE]; Breslauer Strasse 13, 42579 Heiligenhaus (DE). MÜLLER, Ulrich [DE/DE]; Schneegelskothen 7c, 42549 Velbert (DE). PLATE, Jeffrey, D. [US/US]; 9395 North 49th Street, Apt. 201, Brown Deer, WI 53223 (US).
- (74) Anwalt: MENTZEL, Norbert; Kleiner Werth 34, 42275 Wuppertal (DE).
- (81) Bestimmungsstaaten (national): AU, BR, CN, IN, JP, KR, US.
- (84) Bestimmungsstaaten (regional): europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).
- Veröffentlicht:  
— Mit internationalem Recherchenbericht.

[Fortsetzung auf der nächsten Seite]

(54) Title: COMBINED MECHANICAL AND ELECTRONIC KEY, IN PARTICULAR FOR THE LOCKS OF MOTOR VEHICLES

(54) Bezeichnung: KOMBINIERTER MECHANISCHER UND ELEKTRONISCHER SCHLÜSSEL, INSBESONDERE FÜR AN FAHRZEUGEN BEFINDLICHE SCHLÖSSER



(57) Abstract: The invention relates to a combined mechanical and electronic key comprising a key housing for electronic components and an L-shaped flat key (30). Said flat key consists of a bearing limb (31) which enables the key to pivot into a storage position and a shank (32) which mechanically operates the lock. The shank (32) of the flat key (30) can be displaced between an inoperative position, retracted into the key housing and an operative position, in which it projects out of the housing. A push-button preferably also acts as the pivoting axis for the flat key (30). The push-button and the housing have profiled sections and the bearing limb has co-operating profiled sections (37, 38, 39), to subject the flat key (30) to a force in the operative position and to lock the key in one of its positions. The invention aims to produce a simple, cost-effective key. To this end, the flat key is configured as a planar plate (34) with an L-shaped outline, the shank (32) sharing the same plane as the bearing limb. The bearing limb (31) has an opening (35) in the plate for receiving, in a rotationally fixed manner, an insert (36) that has the co-operating profiled section (37 to 39).

[Fortsetzung auf der nächsten Seite]

WO 01/48339 A1



— *Vor Ablauf der für Änderungen der Ansprüche geltenden Frist; Veröffentlichung wird wiederholt, falls Änderungen eintreffen.*

*Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCI-Gazette verwiesen.*

---

**(57) Zusammenfassung:** Bei einem kombinierten mechanischen und elektronischen Schlüssel gibt es sowohl einen Schlüsselbehälter für elektronische Bauteile als auch einen L-förmigen Flachs Schlüssel (30), der einen zu seiner Schwenklagerung dienenden Lagerschenkel (31) und einen zur mechanischen Betätigung des Schlosses dienenden Schaftschenkel (32) besitzt. Der Flachs Schlüssel (30) ist mit seinem Schaftschenkel (32) zwischen einer in den Schlüsselbehälter eingeschwenkten Ruhelage und einer herausgeschwenkten Gebrauchslage bewegbar. Ein Druckknopf dient vorzugsweise zugleich als Schwenkachse für den Flachs Schlüssel (30). Der Druckknopf und der Behälter besitzen Profile und der Lagerschenkel Gegenprofile (37, 38, 39), um den Flachs Schlüssel (30) in seine Gebrauchslage kraftzubelasten und in einer seiner Lagen zu arretieren. Für eine einfachere und kostengünstigere Herstellung wird vorgeschlagen, den Flachs Schlüssel als ebene Platte (34) mit L-förmigem Umrissprofil auszubilden, wo der Schaftschenkel (32) in der gleichen Ebene wie der Lagerschenkel angeordnet ist. Dabei besitzt der Lagerschenkel (31) einen Plattendurchbruch (35), der zur drehfesten Aufnahme eines das Gegenprofil (37 bis 39) aufweisenden Einsatzes (36) dient.



---

Kombinierter mechanischer und elektronischer Schlüssel, insbesondere für an Fahrzeugen befindliche Schlösser

---

Die Erfindung richtet sich auf einen kombinierten Schlüssel der im Oberbegriff des Anspruches 1 angegebenen Art. Ein solcher Schlüssel erlaubt sowohl eine unmittelbare mechanische Betätigung der Schlösser als auch, alternativ oder ergänzend, eine elektronische Betätigung, z.B. eine Fernbedienung dieses Schlosses bzw. auch anderer Schlösser. Der Schlüsselbehälter ist das Handhabungsmittel sowohl zur mechanischen als auch elektrischen Schlüsselbetätigung. Für die elektronische Betätigung besitzt daher der Schlüsselbehälter an seiner Außenseite Betätigungsstellen, z.B. in Form von elektrischen Druckknöpfen oder nachgiebigen Membranen, die auf im Behälterinneren angeordnete elektrische Schalter od. dgl. einwirken. Der mechanische Flachschlüssel ist L-förmig gestaltet und mit seinem einen L-Schenkel am Vorderende des Behälters schwenkbar gelagert, weshalb der „Lagerschenkel“ genannt werden soll. In der Ruhelage befindet sich der Flachschlüssel mit seinem anderen, den Schlüsselschaft bildenden L-Schenkel in einer Einschwenkposition im Behälter. Dieser L-Schenkel soll nachfolgend „Schaftschenkel“ bezeichnet werden. Der Flachschlüssel lässt sich mit seinem Schaftschenkel in eine Gebrauchslage herauschwenken. Zur Lagesicherung empfiehlt es sich den Flachschlüssel in beiden Lagen im Schlüsselbehälter zu arretieren.

Bei dem bekannten Schlüssel der im Oberbegriff von Anspruch 1 genannten Art (EP 0 267 429) ist der L-förmige Flachschlüssel mit seinen Schenkeln zweiteilig

ausgebildet; er besitzt ein Kopfstück in Form eines Lagerrings mit einem tangentialen Ansatz, in welchen das Ende einer Klinge einsteckbar und darin lösbar befestigt ist. Das eingesteckte Kupplungsstück der Klinge muss durch eine Schraube oder einen Niet in der Einstecklage gesichert werden, was mühsam und zeitaufwendig ist. Der den Schaftschenkel bildende L-Schenkel des bekannten Flachschrüssels umfasst den Lagerring, den Ansatz und die eingesteckte Klinge. Der Schaftschenkel ist also zweistückig ausgebildet. Der Übergangsbereich zwischen der eingesteckten Klinge und dem Ansatz am Lagerring ist bruchgefährdet. Um einen Bruch auszuschließen muss das den Aufnahmeschlitz für die Klinge umschließende Material im Ansatz des Lagerrings möglichst dick ausgebildet werden, was der Zielsetzung eines raumsparenden Schlüssels entgegenläuft.

Bei einem bekannten Schlüssel (DE 39 02 537 C2) ist im Schwenkachsenbereich des Flachschrüssels ein mechanischer Druckknopf angeordnet, der axial und radial gefedert ist. Der Druckknopf dient als Schwenkachse für den Flachschrüssel. Die doppelte Fedcrung des Druckknopfes hat zwei Aufgaben beim Flachschrüssel zu erfüllen. Die eine Aufgabe besteht darin, den Flachschrüssel in Schwenkrichtung aus seiner Ruhelage in Richtung seiner Gebrauchslage federzubelasten. Die andere Aufgabe liegt darin, möglichst beide Schwenklagen des Flachschrüssels zu arretieren. Dafür benötigt der Druckknopf geeignete Profilierungen und der Flachschrüssel geeignete Gegenprofilierungen. Zwar ist der Flachschrüssel L-förmig ausgebildet, doch muss der Lagerschenkel wegen der Gegenprofile eine beachtliche Bauhöhe aufweisen und wird gesondert als Lagerkörper mit Vierkantprofil vorgefertigt. Um die große Bauhöhe des Lagerkörpers zu nutzen, ordnete man den Schaftschenkel in einer Parallelebene zur Schwenkachse des Flachschrüssels an. Das erfordert eine entsprechend große Höhendimension im Schlüsselbehälter. Der zur Lagerung des mechanischen Druckknopfs dienende Lagerkörper des Flachschrüssels besitzt einen Schlitz zur nachträglichen Anbringung des für sich gefertigten Schlüsselschafts. Der Schlüsselschaft wird in den Schlitz des Lagerkörpers eingesteckt und dort durch einen Stift od. dgl. gesichert. Das ist zeit- und kostenaufwendig.

Es gibt kombinierte Schlüssel (DE 22 26 385 A; DE 38 42 790 C1), die zwar einen flachen L-förmigen Flachschrüssel aufweisen, doch ist ein Druckknopf im

Achsbereich nicht vorgesehen. Die Schwenkachse erzeugt ein unbeweglicher Lagerstift. Weil kein Gegenprofil für einen Druckknopf erforderlich ist, kann der zur Schwenklagerung dienende Lagerschenkel des Flachprofils flach ausgebildet sein. Man bildet den Flachslüssel als eine ebene Platte aus, in welcher auch das Flachprofil des Schaftschenkels liegt. Dieses Schlüsselgehäuse kann zwar flacher gebaut werden, doch gibt es keine Federbelastung, um den Schaftschenkel aus einer in dem Schlüsselbehälter abgesenkten Ruhelage in seine herausgeschwenkte Gebrauchslage zu überführen. Dies erfordert eine mühsame Handhabung. Außerdem gibt es keine raumsparende Möglichkeit, um den Flachslüssel in diesen Lagen im Behälter zu arretieren. Diese nicht festlegbare Schwenkposition des Flachsüssels bringt Probleme sowohl beim Tragen in der Hosentasche als auch beim Gebrauch, z.B. während der Drehbetätigung des Schlüsselgehäuses.

Bei Schraubverbindungen an Blechprofilen ist es bekannt, zum Erreichen der nötigen Einschraublänge für die Schraube das Muttergewinde im Blechprofil durch ein Ansatzstück oder ein eingewietetes Einsatzstück zu vergrößern (U. Richter, R. v. Voss, F. Kozler: Bauelemente der Feinmechanik, Berlin: Verlag Technik, 1954, S. 137). Diese Ausbildung von Muttergewinden in Blechprofilen steht mit Flachsüsseln in keinem Zusammenhang. Diese Druckschrift gibt keine Anregungen für den Aufbau eines L-förmigen Flachsüssels.

Der Erfindung liegt die Aufgabe zugrunde, einen zuverlässigen, raumsparenden Schlüssel der im Oberbegriff des Anspruches 1 genannten Art zu entwickeln, der sich einfacher und kostengünstiger herstellen lässt. Dies wird erfindungsgemäß durch die im Kennzeichen des Anspruches 1 angeführten Maßnahmen erreicht, denen folgende besondere Bedeutung zukommt.

Bei der Erfindung wird zunächst der Schlüssel mit seinen beiden L-Schenkeln einstückig in Form einer ebenen Platte ausgebildet. Man kann den L-förmigen Flachslüssel aus Plattenmaterial ausstanzen. Durch die einstückige Ausbildung liegt ein stabiler bruchfester Übergang zwischen dem Lagerschenkel und dem Schaftschenkel vor. Trotz der flachen Ausbildung dieses L-förmigen Schlüssel kann im Bereich seines Lagerschenkels der mechanische Druckknopf im Schlüsselbehälter

eingesetzt werden. Dies ist deswegen möglich, weil die für den Druckknopf an sich erforderlichen Gegenprofile einem Einsatz überlassen werden, der in einem Plattendurchbruch des Lagerschenkels drehfest aufgenommen wird. Der Einsatz dient sowohl zur Schwenklagerung als auch zweckmäßigerweise zur Axialführung des Druckknopfs und zur Aufnahme seiner Federmittel. Dadurch ist auch der Aufbau des Schlüsselbehälters vereinfacht. Trotz einer einstückigen, preiswerten L-Plattenform des Flachschlüssels lässt sich seine Arretierung in der Ruhe- und Gebrauchslage über den Druckknopf zuverlässig verwirklichen. Außerdem wird der Schlüssel durch die am Druckknopf und Einsatz vorgesehenen Mitnahmeflächen mittels der auf ihn wirkende Federkraft aus einer Ruhelage in die Gebrauchslage selbsttätig herausgeschwenkt, wenn in der Ruhelage die Arretierung durch Betätigen des Druckknopfs unwirksam gesetzt worden ist.

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 schematisch dargestellt. Es zeigen:

- Fig. 1, in perspektivischer Darstellung, den Schlüsselbehälter mit herausragendem mechanischen Flachschlüssel,
- Fig. 2, ebenfalls in perspektivischer Darstellung, eine zum Flachschlüssel von Fig. 1 gehörende Steckeinheit, bestehend aus einer die elektronischen Bauteile umschließenden Elektrokapsel,
- Fig. 3 ein aus dem Schlüsselbehälter von Fig. 1 und der Steckeinheit von Fig. 2 zusammengestecktes Kombinationsgehäuse, das zur Handhabung bei mechanischer und elektronischer Betätigung des Schlüssels dient,
- Fig. 4, in Explosionsdarstellung, einige wesentliche Bestandteile des in Fig. 1 gezeigten Schlüsselbehälters mit dem mechanischen Flachschlüssel, vor deren Zusammenbau,

- Fig. 5, in Explosionsdarstellung, die beiden Bestandteile des mechanischen Flachschlüssels vor ihrer Vereinigung,
- Fig. 6 einen Querschnitt durch den einen Bestandteil von Fig. 5, längs der dortigen Schnittlinie VI - VI,
- Fig. 7 einen Querschnitt durch das zusammengebaute Schlüsselbehälter von Fig. 1 längs der dortigen Schnittlinie VII - VII, wobei ein Druckknopf in seiner eingedrückten Position gezeigt ist,
- Fig. 8 einen Axialschnitt durch den in Fig. 1 gezeigten Schlüsselbehälter längs der dortigen Schnittlinie VIII - VIII und
- Fig. 9 einen Querschnitt durch das in Fig. 3 gezeigte Kombinationsgehäuse längs der dortigen Schnittlinie IX - IX.

Der kombinierte Schlüssel nach der Erfindung erlaubt sowohl eine mechanische als auch eine elektronische Betätigung eines nicht näher gezeigten Schlosses. Er besteht aus zwei jeweils für sich vorgefertigten Teilen 10, 20, die nachträglich ineinandergefügt werden. Der eine Teil 10 umfasst die mechanischen Schließmittel und besteht aus einem Schlüsselbehälter 10, dessen Bestandteile aus der Explosionsdarstellung von Fig. 4 am besten zu erkennen sind. Der andere Teil 20 ist eine noch näher zu beschreibende Steckeinheit, welche die in ihrem Inneren die im Querschnitt von Fig. 9 angedeuteten elektronischen Bauteile 40 umfasst.

Ausweislich der Fig. 1 und 4 umfasst der mechanische Teil zunächst einen zweischaligen Schlüsselbehälter 10. Während die Oberschale 11, wie Fig. 7 und 8 erkennen lässt, als ebene Platte mit stellenweisen Kupplungsvorsprüngen 13 an ihrer Innenfläche ausgebildet ist, umfasst die Unterschale 12 außer ihrem Schalenboden 15 auch noch Schalenseitenwände 14. In den Schalenseitenwänden 14 befinden sich stellenweise Kupplungsaufnahmen 16 für die vorerwähnten Kupplungsvorsprünge 13 der Oberschale 11. Die Oberschale 11 erstreckt sich nur über einen vorderen Bereich

des Schlüsselbehälters 10 und weist im hinteren Bereich einen Ausbruch 17 auf, der zum Schaleninneren 18 hin einen von außen zugänglichen Freiraum erzeugt. Das ist für das noch näher zu beschreibende Einstecken bzw. Herausziehen der Steckeinheit 20 bedeutungsvoll.

Zum Schlüsselbehälter 10 gehört, wie Fig. 4 zeigt, ein mechanischer Flachs Schlüssel 30 der beweglich angeordnet ist, um aus einer nicht näher gezeigten versenkten Ruhelage im Behälter 10 in eine aus dem Behälter herausragenden, in Fig. 1 bis 4 ersichtliche Gebrauchslage überführt zu werden. Der Flachs Schlüssel 30 besteht aus metallischem Werkstoff. Obwohl auch andere Bewegungen denkbar wären, ist dieser Flachs Schlüssel 30 um die strichpunktiert in den Fig. 1, 3 und 4 angedeuteten Schwenkachsen 33 schwenkbeweglich. Dabei ist der Flachs Schlüssel 30 als ein Stanzling aus einer in Fig. 4 strichpunktiert verdeutlichten ebenen Platte 34 ausgebildet, wobei der Stanzling ein L-förmiges Umrissprofil aus zwei Schenkeln 31, 32 besitzt. Der eine L-Schenkel ist kurz ausgebildet und dient zur Schwenklagerung des Flachs Schlüssels 30 am Vorderende des Schlüsselbehälters 10 und wird daher nachfolgend kurz „Lagerschenkel“ genannt. Der andere L-Schenkel 32 umfasst das eigentliche Flachprofil des Schlüsselschafts, weshalb er nachfolgend als „Schaftschenkel“ bezeichnet werden soll. Beide Schenkel 31, 32 liegen also in einer gemeinsamen, durch den erwähnten Plattenverlauf 34 bestimmten Ebene, die im fertig montierten Zustand des Schlüsselbehälters 10 senkrecht zur Schwenkachse 33 verläuft. Ausweislich der Fig. 5 ist der Lagerschenkel 31 mit einem unrundern Plattendurchbruch 35 versehen, der zur Aufnahme eines besonderen Einsatzes 36 dient.

Der Druckknopf 40 ist sowohl axial als auch radial federbelastet und besitzt mit dem Behälter 10 übereinstimmend ausgebildete Profile 19, 48, 28. Der Einsatz 36 besteht aus relativ nachgiebigem Material, vorzugsweise Kunststoff und besitzt ein besonderes Gegenprofil 37, 38, 39 für einen die Lage der Schwenkachse 33 bestimmenden Druckknopf 40. Die Federwirkung übernimmt eine kombinierte Druck-Dreh-Feder 41, die, ausweislich der Fig. 7, in einer Axialbohrung 45 des Druckknopfs 40 aufgenommen ist. Die Feder 41 ist mit ihrem einen Federende 42 drehfest mit dem Druckknopf 40 verbunden, während ihr anderes Federende 43 in der

Unterschale 12 des Behälters 10 festgehalten wird. Die Feder 41 ist wendelförmig ausgebildet. Im Montagefall greift ein an der bodenseitigen Innenfläche der Unterschale 12 sitzender Dorn 44 sowohl ins Wendelinnere hinein, als auch in den Einsatz 36 ein.

Gemäß Fig. 5 wird zunächst der Flachs Schlüssel 30 mit seinem Plattendurchbruch 35 durch Stanzen erzeugt und dann, nachträglich, der Einsatz 36 in den Plattendurchbruch 35 vertikal eingesteckt. Nach diesem Einstecken ragt, wie Fig. 4 und 7 zeigen, über die beiden Plattenflächen des Flachs Schlüssels heraus. Dazu gehören zylindrische Ansätze 47, gemäß Fig. 6, aber auch ein Anschlagzapfen 39 an beiden Flächenseiten, der in ein Ringnutsegment 19 der beiden Schalen 11 und 12 hineinragt, wie aus Fig. 8 zu entnehmen ist. In der in Fig. 8 ausgezogen gezeichneten Position des Anschlagnockens 39 liegt die bereits eingangs erwähnte, aus dem Behälter 10 herausgeschwenkte Gebrauchslage vor. Dann erstreckt sich der vorbeschriebene Schaftschenkel 32 des Flachs Schlüssels 30 in Richtung der in Fig. 8 strichpunktirt angedeuteten Hilfslinie 30.1, welche die in den übrigen Fig. dargestellte Gebrauchslage des Flachs Schlüssels 30 kennzeichnet. In dieser Gebrauchslage 30.1 ist der Flachs Schlüssel durch den Druckknopf 40 arretiert. Dann greifen am Druckknopf 40 vorgesehene, hier diametral angeordnete Mitnahmeflügel 48 in zugehörige Radialnuten 28 an der Innenfläche der Oberschale 11 hinein und sichern so die Ausschwenklage des Flachs Schlüssels 30.

Die Mitnahmeflügel 48 besitzen, als Gegenprofil, im Einsatz 36 Axialnuten 48, die eine Eindruckbewegung im Sinne des aus Fig. 7 erkennbaren Kraftpfeils 46 zulassen. Diese Eindruckbewegung 46, die in Fig. 7 vollzogen ist, führt zu einer axialen Absenkung des Druckknopfs 40, wodurch die Mitnahmeflügel 48 die Radialnuten 28 freigeben. Die Eindruckbewegung 46 erfolgt gegen die axiale Kraftwirkung der Feder 41. Die Arretierung der Gebrauchslage 30.1 ist dann aufgehoben. Der Flachs Schlüssel kann dann im Sinne des Bewegungspfeils 29 von Fig. 8 gegen die durch den Kraftpfeil 49 in Fig. 8 verdeutlichte Drehkraft der Feder 41 in seine Ruhelage im Gehäuse zurückgeschwenkt werden. Dann liegt der Schaftschenkel 32 des Flachs Schlüssels 30, in Fig. 8 gesehen, an der dort mit 30.2 gekennzeichneten Strichpunktlinie. In dieser Ruhelage 30.2 verschwindet der Schaftschenkel 32 in

einem aus Fig. 3 erkennbaren seitlichen Spalt 24 eines noch näher zu beschreibenden Gesamtgehäuses 50, welches aus dem Schlüsselbehälter 10 und der darin eingeschobenen Steckeinheit 20 entsteht. Dann sind die Mitnahme­flügel 48 wieder in axialer Ausrichtung mit den gehäuse­seitigen Radialnuten 28, wo sie durch die Rückstellkraft der Feder 41 einschnappen und so auch diese Ruhelage 30.2 des Flachs­schlüssels 30 im Schlüsselbehälter 10 arretieren.

Bei der Schwenkbewegung 29 dient der Druckknopf 40 auch als Schwenklager. Dazu ist in der Oberschale 11 des Behälters 10 eine aus Fig. 4 erkennbare Lagerbohrung 25 vorgesehen. Diese ist in axialer Ausrichtung mit einer in Fig. 5 und 6 gezeigten Axialbohrung 37 des Einsatzes 36 und mit dem bereits mehrfach erwähnten Dorn 44 der Unterschale 12. Der Druckknopf 40 bestimmt die Schwenkachse 33 des Flachs­schlüssels 30. Der Anschlagzapfen 39 vom Einsatz 36 einerseits und das ihm gehäuse­seitig zugeordnete Ringnutsegment 19 andererseits können auch Dreh­führungsfunktionen bei der Schwenkbewegung 29 übernehmen. Außerdem können Dreh­anschläge durch das Umrissprofil des Schlüssels 30 einerseits und Innenflächen an den beiden Schalen 11, 12 andererseits verwirklicht sein.

Statt einer Vorfertigung des Einsatzes 36 könnte man den Einsatz 36 durch eine Spritzgusstechnik nachfertigen. Dazu wird der beschriebene Flachs­schlüssel 30 in eine Spritzgussform eingebracht, in welcher dann der Einsatz 36 im Plattendurchbruch 35 durch Gießen gebildet wird. Die erwähnte Gegenprofilierung 37, 38, 39, 47 liegt dann in ähnlicher Form vor.

In manchen Anwendungsfällen ist bei dem eingangs erwähnten kombinierten Schlüssel für die elektronische Betätigung auch ein sogenannter Transponder 26 erwünscht. Dieser Transponder 26 soll bereits zur elektronischen Individualisierung dieses kombinierten Schlüssels sorgen. Wird dieser Schlüssel in das zugehörige Schloss eingesteckt, so findet zwischen dem Transponder 26 und dem Schloss eine Kommunikation statt, die bei Übereinstimmung von Schloss und Schlüssel bereits Schlossfunktionen auslöst. Deswegen werden bei der Erfindung derartige Transponder 26 im vorderen Bereich des Schlüsselbehälters 10 untergebracht. Dazu besitzt die Unterschale 12 eine Kammer 27, in welche der bzw. die Transponder 26



eingeklebt werden können. Weil eine elektronische Energieversorgung der Transponder 26 nicht erforderlich ist, braucht der fertig montierte Schlüsselbehälter 10 von Fig. 1 nicht mehr in seine Schalen 11, 12 zerlegt zu werden, um dort einen Batteriewechsel od. dgl. vorzunehmen. Die Transponder 26 sind also in der Kammer 27 permanent geschützt. Das gilt auch für die bereits eingangs erwähnten weiteren elektronischen Bauteile 21, welche innerer Bestandteil der bereits erwähnten lösbaren Steckeinheit 20 des Gesamtgehäuses 50 sind.

Wie am besten aus Fig. 9 zu ersehen ist, gehören zur Steckeinheit 20 eine gehäuseartige Kapsel 22, in deren Innenraum 23 die Bauteile 21 angeordnet und so nach außen allseitig abgeschlossen sind. Im Kapselinneren 23 können auch die Schaltungen der Bauelemente und gegebenenfalls die elektrische Störung angeordnet sein. Diese Baueinheit 21, 22, die als Steckeinheit mit dem Schlüsselbehälter 10 fungiert, wird komplett vorgefertigt und soll nachfolgend „Elektrokapsel“ genannt werden. Dazu ist der Schlüsselbehälter 10 profilmäßig in folgender Weise angepasst.

Der eingangs erwähnte Ausbruch 17 im Schlüsselbehälter 10 erfolgt einfach dadurch, dass die Oberschale 11, gemäß Fig. 1, nur den Vorderabschnitt 51 des Schlüsselbehälters 10 überdeckt. Dadurch ist ein von außen zugänglicher Freiraum ins Schaleninnere 18 erzeugt. Dieser Freiraum 17 besitzt nicht nur eine nach oben weisende Oberöffnung 52, sondern erstreckt sich auch in eine vom Hinterende 54 zugängliche Seitenöffnung 53. Diese entsteht, weil nicht nur der hintere Abschnitt der Oberschale 11 fehlt, sondern auch, wie Fig. 1 zeigt, die Seitenwand 14 der Unterschale 12 am Hinterende 54 des Behälters 10 weggefallen ist. Die Elektrokapsel 20 wird durch diese Seitenöffnung 53 in den Freiraum 17 des Schlüsselbehälters 10 gemäß dem Bewegungspfeil 55 von Fig. 1 eingeschoben. In ihrer Einschublage, gemäß Fig. 3, verschließt die Elektrokapsel 20 die Oberöffnung 52. Die Einschubbewegung 55 ist in einer Parallelebene zu der oben erwähnten Schwenkbewegung 29 angeordnet. Dabei sind folgende Führungsmittel 61, 62 zum gezielten Einstecken und Verschieben 55 der Elektrokapsel 20 vorgesehen.

An der Innenfläche des Schalenbodens 15 der Unterschale 12 befinden sich zwei parallele Führungsleisten 61, die zur Seitenöffnung 53 hin gerichtet sind. Sie sind

hinterschnitten und besitzen vorzugsweise ein schwalbenschwanzförmiges Profil. Ihnen sind angepasste Führungsnuten 62 an der Unterseite des Gehäuses der Elektrokapsel 20 zugeordnet. Die Eingriffslage dieser Führungsmittel 61, 62 ist im Schnitt von Fig. 9 zu erkennen. Dabei ist die eine Längsseite vom Kapselgehäuse 22 gemäß Fig. 9 bei 58 gestuft, so dass mit einer entsprechenden Stufung 59 in der Unterschale 12, gemäß Fig. 4, in der Einschublage der seitliche Spalt 24 für den Schaftschenkel 32 des Flachschlüssels 30 entsteht. In der Einschublage gemäß Fig. 3 und 9 gehen die sichtbar bleibenden Außenflächen der Elektrokapsel 20 einerseits und des Schlüsselbehälters 10 andererseits ineinander bündig über. Beide Teile 10, 20 bilden dann das bereits erwähnte Kombinationsgehäuse 50, welches beim Handhaben des Schlüssels mit der Hand gemeinsam umgriffen wird und daher „Kombinationsgehäuse“ genannt werden soll. Dies gilt sowohl bei einer mechanischen Betätigung des zugehörigen Schlosses, wo der herausgeschwenkte Schaftschenkel 32 mittels des Kombigehäuses 50 gedreht wird, als auch bei der elektronischen Betätigung. Dafür sind Betätigungsstellen 60 an die sichtbar bleibende Außenfläche der Elektrokapsel 20 im gemeinsamen Kombinationsgehäuse 50 vorgesehen. Diese können aus Druckschaltern oder membranartigen Betätigungsstellen entstehen. Diese Betätigungsstellen können mit weiteren membranartigen Überdeckungen im Bereich des vorerwähnten Druckknopfs 40 vorgesehen sein, dem noch folgende besondere Bedeutung zukommt.

Die in Fig. 3 und 9 gezeigte Einstecklage der Elektrokapsel 20 im Schlüsselbehälter 10 ist nicht nur durch Anschlagmittel begrenzt, sondern auch durch Rastmittel gesichert. Diese Funktion kann in vorteilhafterweise auch vom Druckknopf 40 übernommen werden. Dazu ist die Elektrokapsel 20, gemäß Fig. 2, vorderendig mit einem Lappen 56 verlängert, der in der Einschublage von Fig. 3 den verbliebenen Vorderabschnitt 51 der Oberschale 11 vom Schlüsselbehälter 10 überdeckt. Der Lappen 56 besitzt eine Ausnehmung 57, in welche der axial federnde Druckknopf 40 in der Einschublage der Elektrokapsel 20 gemäß Fig. 3 einschnappt. Dadurch ist der Zusammenhalt des Schlüsselbehälters mit der Elektrokapsel 20 sichergestellt. Die Ausnehmung 57 durchsetzt den Lappen 56, weshalb im Eingriffsfall gemäß Fig. 3 der Druckknopf 40 mit einem zu seiner Betätigung ausreichenden Längenstück aus dem Lappen 56 herausragt. Zur Demontage des Kombinationsgehäuses 50 in seine

Bestandteile 10, 20 wird der Druckknopf 40, wie Fig. 7 zeigt, soweit im Sinne des Pfeils 46 eingedrückt, dass er die Ausnehmung 57 im Lappen 56 freigibt.

Der Druckknopf 40 kann durch eine Membran im Bereich des Lappens 56 überdeckt sein, welche in ähnlicher Weise wie die Betätigungsstellen 61 fungiert. Diese Membrane dieser Betätigungsstellen 61 können mit der vorgenannten Membran im Bereich des Druckknopfs 40 kombiniert sein.

## Bezugszeichenliste :

- 10 erster Schlüsselteil, Schlüsselbehälter
- 11 Oberschale von 10
- 12 Unterschale von 10
- 13 Kupplungsvorsprung an 11
- 14 Schalenseitenwand von 12
- 15 Schalenboden von 12
- 16 Kupplungsaufnahme von 12
- 17 Ausbruch von 11, Freiraum in 18
- 18 Schaleninneres
- 19 Profil in 11, 12 für 39, Ringnutsegment
- 20 zweiter Schlüsselteil, Steckeinheit, Elektrokapsel
- 21 elektronischer Bauteil
- 22 gehäuseartige Kapsel für 21
- 23 Kapselinneres für 22 in 21
- 24 seitlicher Spalt in 50 für 32 (Fig. 3, 9)
- 25 Lagerbohrung in 11 für 40 (Fig. 4)
- 26 Transponder
- 27 Kammer in 11 für 26 (Fig. 4)
- 28 Profil in 11 für 48 von 40, Radialnut (Fig. 7)
- 29 Schwenkbewegungspfeil für 30 (Fig. 8)
- 30 mechanischer Flachschlüssel für 10, Stanzling
- 30.1 Gebrauchslage von 32 (Fig. 8)
- 30.2 Ruhelage von 32 (Fig. 8)
- 31 erster L-Schenkel von 30, Lagerschenkel
- 32 zweiter L-Schenkel von 30, Schaftschenkel
- 33 Schwenkachse für 30
- 34 ebene Platte für 30
- 35 Plattendurchbruch
- 36 Einsatz in 35
- 37 Gegenprofil in 36, Axialbohrung (Fig. 5, 6)

- 38 Gegenprofil von 36, Axialnut in 36 für 48 (Fig. 5, 8)
- 39 Gegenprofil von 36, Führungs- bzw. Anschlagzapfen (Fig. 5, 6)
- 40 Druckknopf
- 41 Druck-Dreh-Feder von 40
- 42 erstes Federende von 41 (Fig. 7)
- 43 zweites Federende von 41 (Fig. 7)
- 44 Dorn an 12 für 41 (Fig. 4)
- 45 Axialbohrung in 40 für 41
- 46 Pfeil der Eindruckbewegung von 40 (Fig. 7)
- 47 Gegenprofil an 36, zylindrischer Ansatz an 36 (Fig. 5)
- 48 Profil, Mitnahme Flügel an 40
- 49 Pfeil der Ausschwenkkraft von 41 für 30 (Fig. 8)
- 50 Gesamtgehäuse aus 10, 20, Kombinationsgehäuse
- 51 Vorderabschnitt von 10
- 52 Oberöffnung von 10 bei 17 (Fig. 1)
- 53 Seitenöffnung von 11 (Fig. 1)
- 54 Hinterende von 10
- 55 Pfeil der Einschubbewegung von 20 in 10 (Fig. 1)
- 56 Lappen an 20 (Fig. 2)
- 57 Ausnehmung in 56 für 40 (Fig. 2)
- 58 Innenstufung von 22 für 24 (Fig. 2, 9)
- 59 Stufe von 12 für 24 (Fig. 4)
- 60 Betätigungsstelle an 20 (Fig. 1)
- 61 Führungsmittel an 12, Führungsleiste
- 62 Führungsmittel an 20, Führungsnut

## P a t e n t a n s p r ü c h e :

- 1.) Kombiniertes mechanischer und elektronischer Schlüssel, insbesondere für in Fahrzeugen befindliche Schlösser,

mit einem gemeinsamen, bei der Schlüsselbetätigung zu handhabenden Schlüsselbehälter (10) sowohl für elektronische Bauteile (21) zur elektronischen Betätigung des Schlosses als auch für einen L-förmigen Flachs Schlüssel (30) zur mechanischen Betätigung des Schlosses,

wobei der Flachs Schlüssel (30) mit seinem einen L-Schenkel, dem Lagerschenkel (31), am Vorderende (51) des Behälters (10) schwenkgelagert (33) ist,

wobei sein anderer, den eigentlichen Schlüsselschaft mit Flachprofil bildender L-Schenkel, der Schaftschenkel (32), aus einer im Behälter (10) eingeschwenkten Ruhelage (30.2) in eine herausgeschwenkte Gebrauchslage (30.1) bewegbar ist,

mit einer axial und radial wirksamen Federbelastung (41)

und mit einem Druckknopf (40), der vorzugsweise zugleich die Schwenkachse (33) des Flachs Schlüssels (30) im Schlüsselbehälter (10) bestimmt,

wobei der Druckknopf (40) und der Behälter (10) Profile (48, 28) aufweisen und der Lagerschenkel (31) Gegenprofile (37, 38, 39, 47) besitzt, durch die der Flachs Schlüssel (30) einerseits in seine Gebrauchslage (30.1) kraftbelastet und andererseits in wenigstens einer seiner Lagen (30.1; 30.2) arretiert wird,

und der Schaftschenkel (32) in der gleichen, senkrecht zur Schwenkachse (33) verlaufenden Ebene angeordnet ist, wie der mit dem Druckknopf (44) zusammenwirkende Lagerschenkel (31),

dadurch gekennzeichnet ,

dass der L-förmige Flachschlüssel (30) mit seinen beiden Schenkelenden (31, 32) als einstückige ebene Platte ausgebildet ist,

dass der Lagerschenkel (31) einen unrunder Plattendurchbruch (35) besitzt

und dass der Plattendurchbruch (35) zur drehfesten Aufnahme eines Einsatzes (36) dient, der ein Gegenprofil (37, 38, 39, 47) aufweist.

2.) Schlüssel nach Anspruch 1, dadurch gekennzeichnet, dass der L-förmige Flachschlüssel (30) und sein unrunder Plattendurchbruch (35) durch Stanzen aus dem Plattenmaterial (34) erzeugt sind und einen Stanzling bildet.

3.) Schlüssel nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass der Einsatz (36) mit seinem Gegenprofil (37, 38, 39, 47) als Vorprodukt herstellbar ist und einen unrunder Umriss aufweist,

und dass der Einsatz (36) nachträglich in den Plattendurchbruch (35) eingesteckt und dort kraft- und/oder formschlüssig festgehalten ist.

4.) Schlüssel nach einem oder mehreren der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass der Flachschlüssel (30) aus einem relativ formfesten, metallischen Material gebildet ist und der Einsatz (36) aus relativ nachgiebigem Material, vorzugsweise Kunststoff besteht.

- 5.) Schlüssel nach einem oder mehreren der Ansprüche 1 bis 4, dadurch gekennzeichnet, dass der Einsatz (36) mindestens eine der beiden Plattenflächen des Flachschlüssels (30) wenigstens bereichsweise überragt.
- 6.) Schlüssel nach Anspruch 1, 2 oder 4, dadurch gekennzeichnet, dass der Einsatz (36) im Bereich des Plattendurchbruchs (35) durch Spritzgusstechnik angeformt und mit dem Flachschlüssel (30) spritzgusstechnisch verbunden ist.
- 7.) Schlüssel nach einem oder mehreren der Ansprüche 1 bis 6, dadurch gekennzeichnet, dass das Gegenprofil vom Einsatz (36) ein axial abragendes Drehanschlag- und/oder Drehführungs-Element (39) aufweist  
  
und dass das Drehanschlag- und/oder Drehführungs-Element im Montagefall in ein Ringnut-Segment (19) an der Innenfläche des Schlüsselgehäuses (10) hineinragt.
- 8.) Schlüssel nach einem oder mehreren der Ansprüche 1 bis 7, dadurch gekennzeichnet, dass das Gegenprofil des Einsatzes (36) eine Axialbohrung (37) mit wenigstens einer davon radial abragenden Axialnut (38) umfasst, in welche der Druckknopf (40) mit mindestens einem abgesetzten Mitnahmeflügel (48) zeitweise und/oder bereichsweise eingreift.



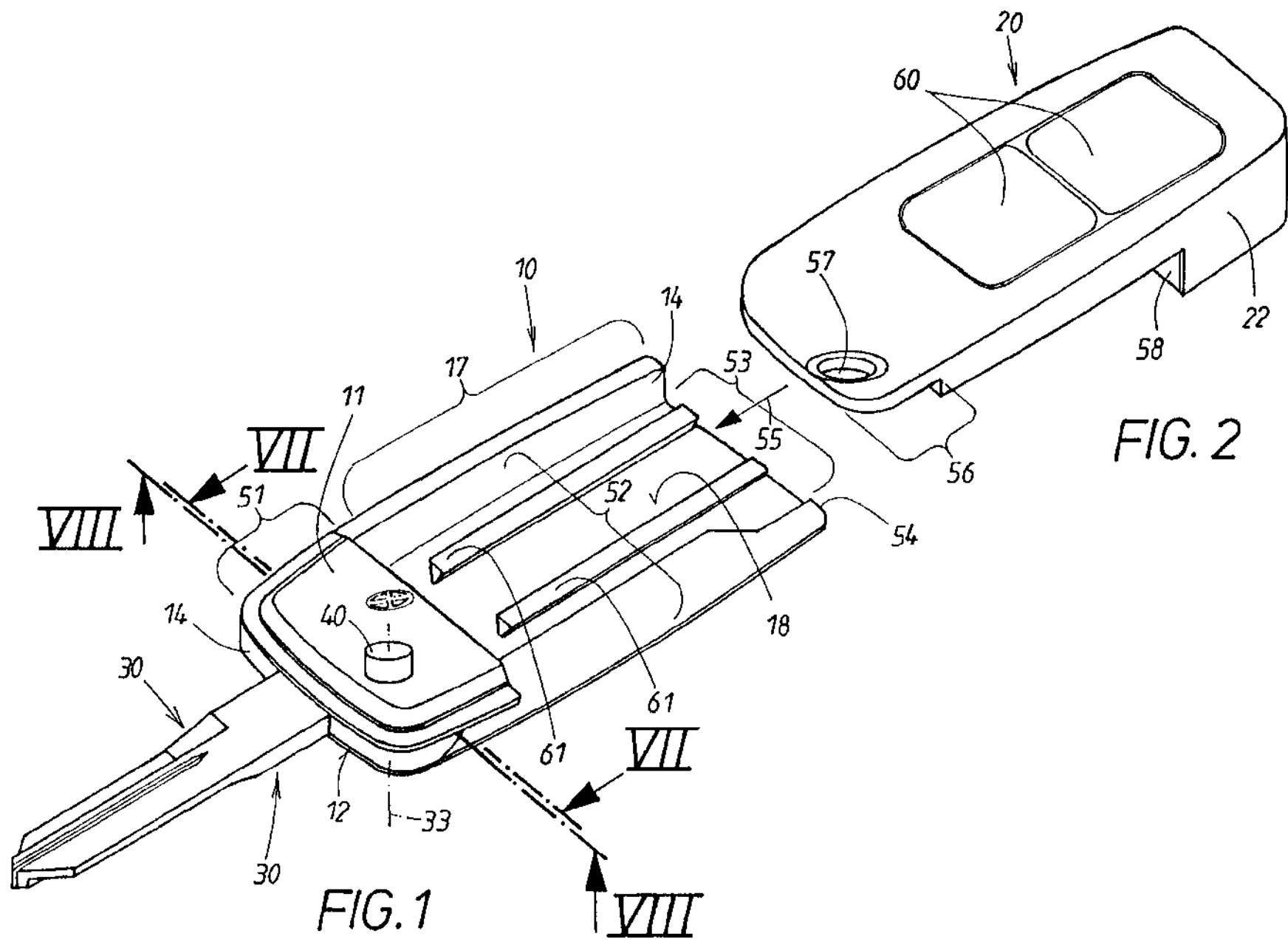


FIG. 2

FIG. 1

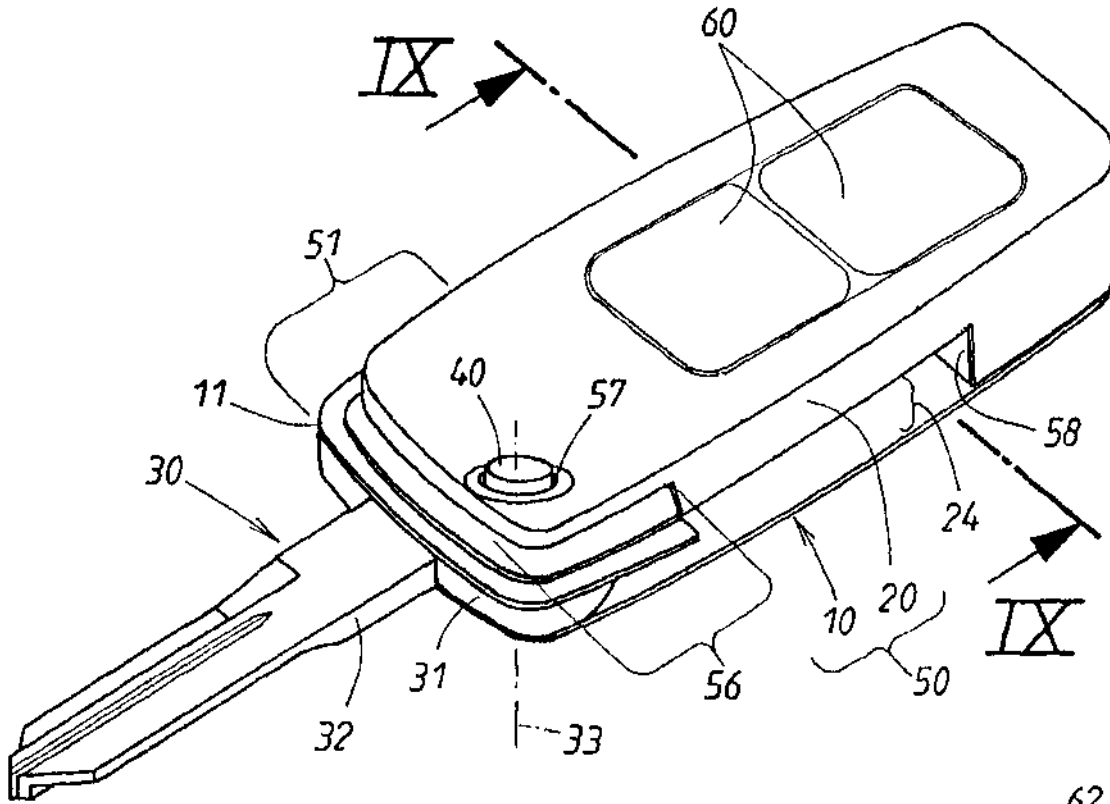


FIG. 3

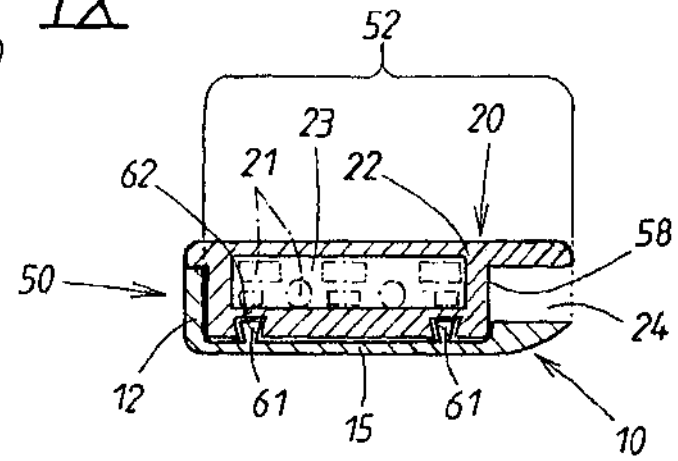


FIG. 9

315

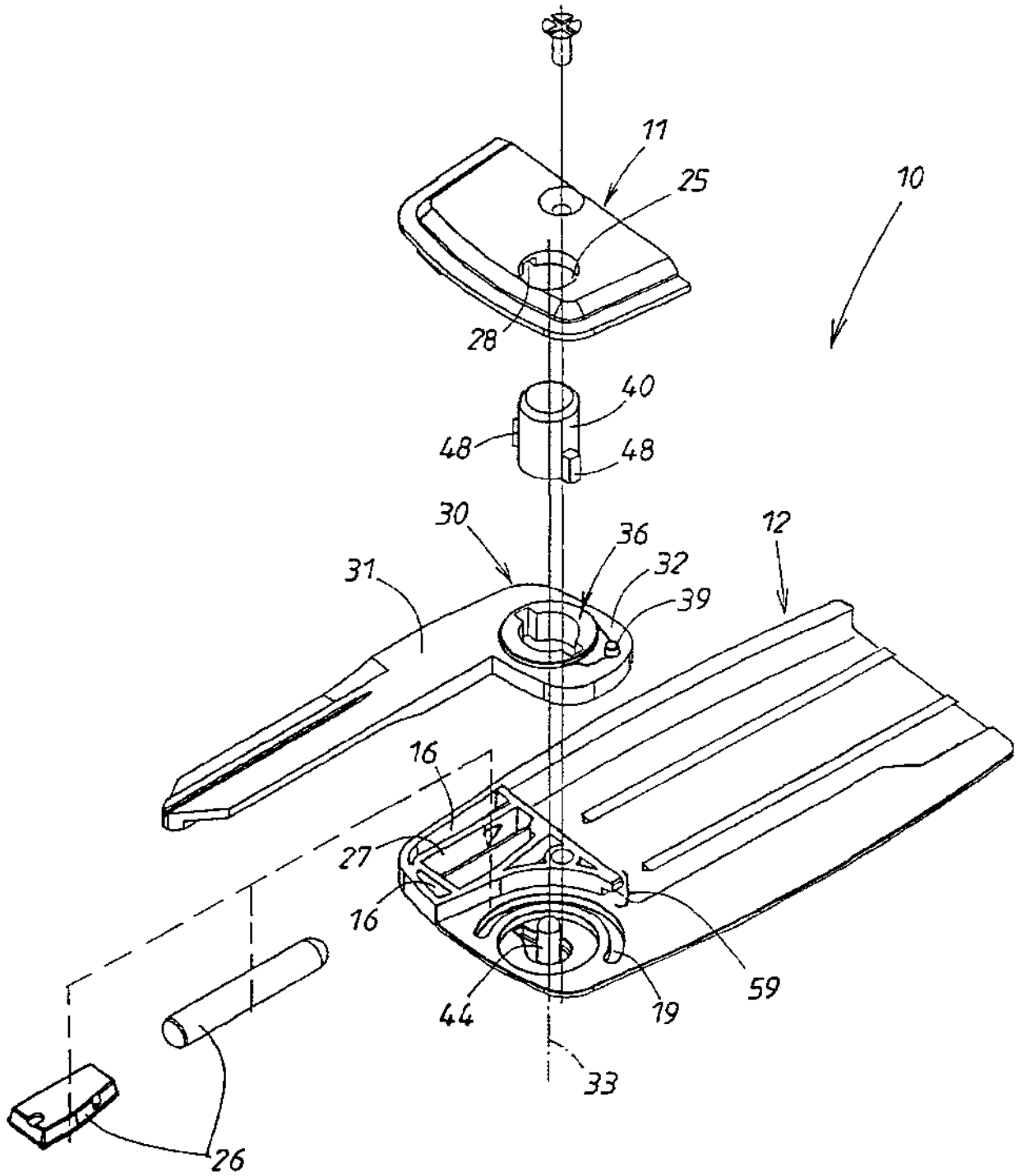
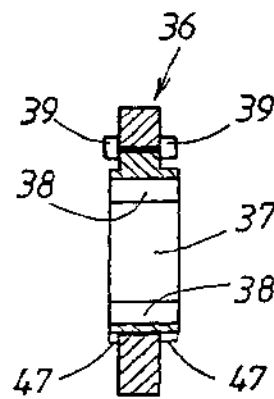
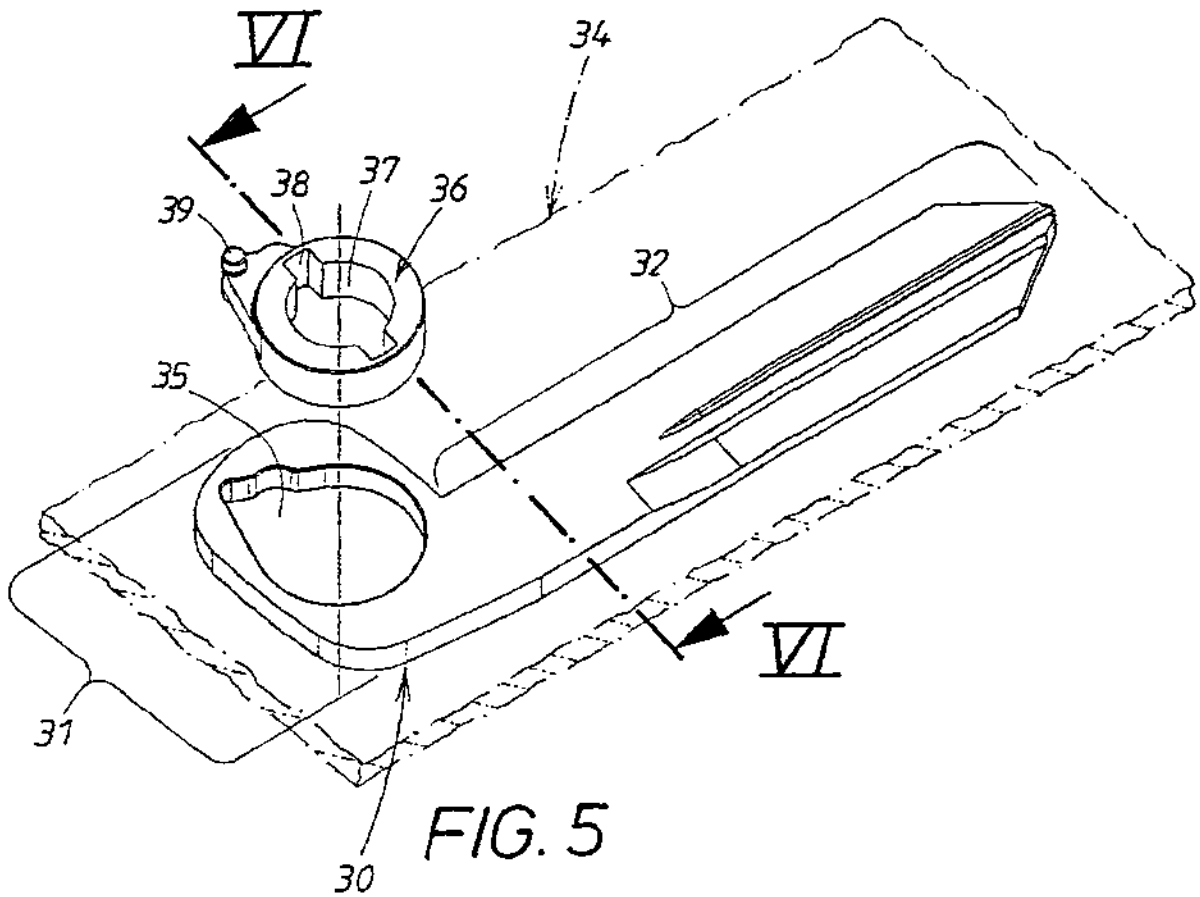


FIG. 4

415



515

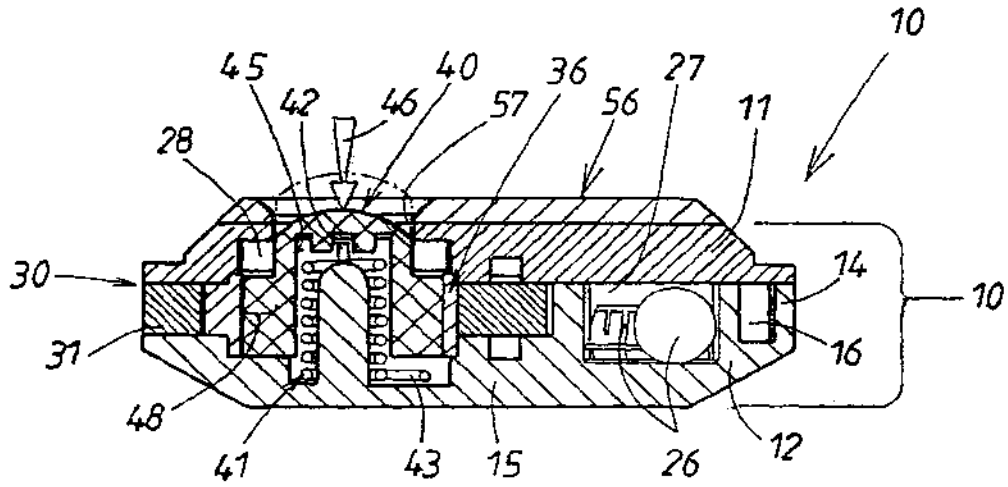


FIG. 7

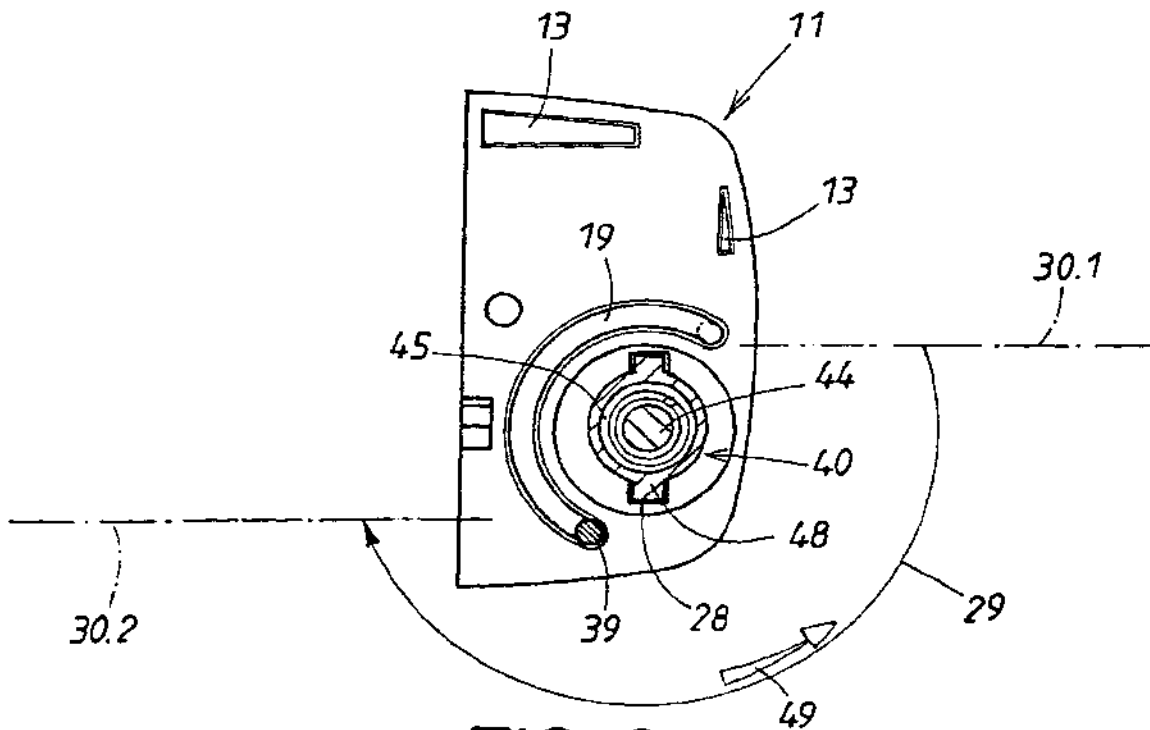


FIG. 8

# INTERNATIONAL SEARCH REPORT

Internatic    Application No  
PCT/EP 00/11619

**A. CLASSIFICATION OF SUBJECT MATTER**  
IPC 7    E05B19/04    E05B49/00

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)

EPO-Internal, WPI Data, PAJ

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE 42 26 579 A (MERCEDES-BENZ AG) 17 February 1994 (1994-02-17) column 4, line 38 -column 4, line 67; figures	1
A	WO 97 17863 A (POWELL) 22 May 1997 (1997-05-22) page 8, line 30 -page 11, line 14; figures	1
P, A	EP 0 985 788 A (VALEO ELECTRONIQUE) 15 March 2000 (2000-03-15) abstract; figures	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.
- \*Z\* document member of the same patent family

Date of the actual completion of the international search

17 May 2001

Date of mailing of the international search report

29/05/2001

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

Vacca, R

# INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No

PCT/EP 00/11619

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
DE 4226579 A	17-02-1994	NONE	
WD 9717863 A	22-05-1997	AU 7579796 A	05-06-1997
EP 985788 A	15-03-2000	FR 2783011 A	10-03-2000

**INTERNATIONALER RECHERCHENBERICHT**

Internationales Aktenzeichen

PCT/EP 00/11619

<b>A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES</b> IPK 7 E05B19/04 E05B49/00		
Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK		
<b>B. RECHERCHIERTE GEBIETE</b> Recherchierte 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) EPO-Internal, WPI Data, PAJ		
<b>C. ALS WESENTLICH ANGESEHENE UNTERLAGEN</b>		
Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	DE 26 579 A (MERCEDES-BENZ AG) 17. Februar 1994 (1994-02-17) Spalte 4, Zeile 38 - Spalte 4, Zeile 67; Abbildungen	1
A	WO 97 17863 A (POWELL) 22. Mai 1997 (1997-05-22) Seite 8, Zeile 30 - Seite 11, Zeile 14; Abbildungen	1
P, A	EP 0 985 788 A (VALEO ELECTRONIQUE) 15. März 2000 (2000-03-15) Zusammenfassung; Abbildungen	1
<input type="checkbox"/> Weitere Veröffentlichungen sind der Fortsetzung von Feld C zu entnehmen <input checked="" type="checkbox"/> 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 erfinderscher Tätigkeit beruhend betrachtet werden *Y* Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfinderscher 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 *Z* Veröffentlichung, die Mitglied derselben Patentfamilie ist		
Datum des Abschlusses der internationalen Recherche 17. Mai 2001		Absenddatum des internationalen Recherchenberichts 29/05/2001
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 Vacca, R



# INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP 00/11619

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(er) der Patentfamilie	Datum der Veröffentlichung
DE 4226579 A	17-02-1994	KEINE	
WO 9717863 A	22-05-1997	AU 7579796 A	05-06-1997
EP 985788 A	15-03-2000	FR 2783011 A	10-03-2000

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum  
Internationales Büro



(43) Internationales Veröffentlichungsdatum  
5. Juli 2001 (05.07.2001)

PCT

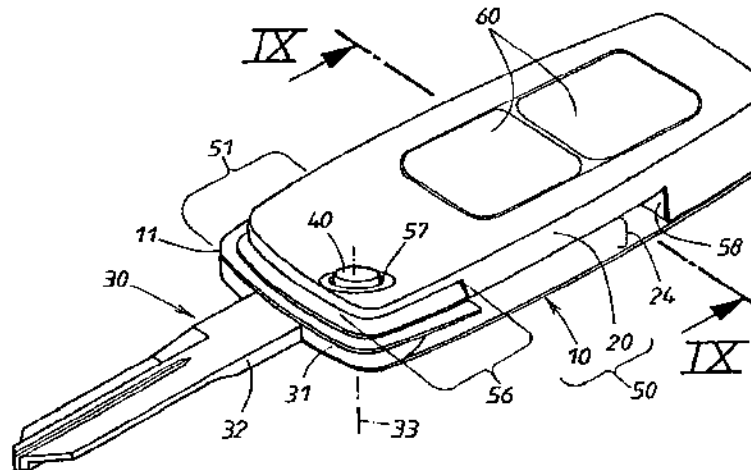
(10) Internationale Veröffentlichungsnummer  
WO 01/48342 A1

- (51) Internationale Patentklassifikation<sup>7</sup>: E05B 49/00, 19/00, 19/04 (72) Erfinder; und  
(75) Erfinder/Anmelder (nur für US): JACOB, Dirk [DE/DE]; Breslauer Strasse 13, 42579 Heiligenhaus (DE). MÜLLER, Ulrich [DE/DE]; Schnegelskothen 7C, 42549 Velbert (DE).
- (21) Internationales Aktenzeichen: PCT/EP00/12431 (74) Anwalt: MENTZEL, Norbert; Kleiner Werth 34, 42275 Wuppertal (DE).
- (22) Internationales Anmeldedatum: 8. Dezember 2000 (08.12.2000) (81) Bestimmungsstaaten (national): AU, BR, CN, IN, JP, KR, US.
- (25) Einreichungssprache: Deutsch (84) Bestimmungsstaaten (regional): europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).
- (30) Angaben zur Priorität: 199 62 976.5 24. Dezember 1999 (24.12.1999) DE (84) Bestimmungsstaaten (regional): europäisches Patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, TR).
- (71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von US): HUF HÜLSBECK & FÜRST GMBH & CO. KG Veröffentlicht:  
[DE/DE]; Steeger Strasse 17, 42551 Velbert (DE). Mit internationalem Recherchenbericht.

[Fortsetzung auf der nächsten Seite]

(54) Title: COMBINED MECHANICAL AND ELECTRONIC KEY, IN PARTICULAR FOR LOCKS IN A VEHICLE

(54) Bezeichnung: KOMBINIERTER MECHANISCHER UND ELEKTRONISCHER SCHLÜSSEL, INSBESONDERE FÜR AN FAHRZEUGEN BEFINDLICHE SCHLÖSSER



(57) Abstract: In a combined mechanical and electronic key, electronic components and mechanical flat keys (30) are normally housed in a common key holder (10). In order to place the flat key (30) between a lowered rest position in a holder (10) and a projecting in-use position, the flat key (30) is movably located in a container (10) and secured in at least one of said positions by a push button (40). The key container is assembled from an upper and a lower shell. In order to avoid sealing problems between both shells, according to the invention, the upper shell (11) is provided with an outbreak in a region pertaining thereto which lies outwith the push button. The outbreak creates a void chamber which can be accessed from the outside and is located on the inside of the shell interior. Said electronic components are enclosed by a housing-like capsule and form therewith a prefabricated electrocapsule (20). The electrocapsule (20) forms a socket unit, which can be inserted thereafter in the void chamber pertaining to the pre-assembled key container (10). The electrocapsules (10) are secured in the key container (10) when inserted in said socket. The push button (40) is used to advantage for securing.

[Fortsetzung auf der nächsten Seite]

IPR2022-00412

Apple EX1043 Page 630



WO 01/48342 A1



*Zur Erklärung der Zweibuchstaben-Codes, und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCF-Gazette verwiesen.*

---

**(57) Zusammenfassung:** Bei einem kombinierten mechanischen und elektronischen Schlüssel sind normalerweise die elektronischen Bauteile und der mechanische Flachs Schlüssel (30) in einem gemeinsamen Schlüsselbehälter (10) untergebracht. Um den Flachs Schlüssel (30) zwischen einer im Behälter (10) versenkten Ruhelage und einer herausragenden Gebrauchslage zu überführen, ist der Flachs Schlüssel (30) im Behälter (10) beweglich aufgenommen und in wenigstens einer dieser Lagen durch einen Druckknopf (40) arretiert. Der Schlüsselbehälter wird aus einer Ober- und Unterschale montiert. Um Dichtungsprobleme zwischen den beiden Schalen zu vermeiden, schlägt die Erfindung vor, die Oberschale (11) in ihrem ausserhalb des Druckknopfs (40) liegenden Bereich mit einem Ausbruch zu versehen. Der Ausbruch erzeugt einen von aussen zugänglichen Freiraum im Schaleninneren. Die elektronischen Bauteile sind von einer gehäuseartigen Kapsel umschlossen und bilden mit dieser eine vorgefertigte Elektrokapsel (20). Die Elektrokapsel (20) bildet eine Steckereinheit, welche nachträglich in den Freiraum des fertig montierten Schlüsselbehälters (10) einsteckbar ist. Im Einsteckfall ist die Elektrokapsel (20) im Schlüsselbehälter (10) gesichert. Vorteilhaft nutzt man den Druckknopf (40) für diese Sicherung aus.

---

Kombinierter mechanischer und elektronischer Schlüssel, insbesondere für an Fahrzeugen befindliche Schlösser

---

Die Erfindung richtet sich auf einen kombinierten Schlüssel der im Oberbegriff des Anspruches 1 angegebenen Art. Ein solcher Schlüssel erlaubt sowohl eine unmittelbare mechanische Betätigung der Schlösser als auch, alternativ oder ergänzend, eine elektronische Betätigung, z.B. eine Fernbedienung dieses Schlosses bzw. auch anderer Schlösser. Der Schlüsselbehälter ist das Handhabungsmittel sowohl zur mechanischen als auch elektrischen Schlüsselbetätigung. Für die elektronische Betätigung besitzt daher der Schlüsselbehälter an seiner Außenseite Betätigungsstellen, z.B. in Form von elektrischen Druckknöpfen oder nachgiebigen Membranen, die auf im Behälterinneren angeordnete elektrische Schalter od. dgl. einwirken. Der mechanische Flachslüssel ist im Behälter beweglich aufgenommen und kann aus einer im Behälter versenkten Ruhelage in einer aus dem Behälter herausragenden Gebrauchslage überführt werden. Zur Lagesicherung empfiehlt es sich den Flachslüssel in beiden Lagen durch einen im Behälter angeordneten axial gefederten Druckknopf zu arretieren.

Bei dem bekannten Schlüssel dieser Art (DE 39 02 537 C2) sind im Inneren des Schlüsselbehälters nicht nur der mechanische Flachs Schlüssel sondern auch die elektronischen Bauteile für die elektronische Betätigung unmittelbar angeordnet. Die elektronischen Bauteile umfassen auch die zur Energieversorgung dienenden Batterien, die nach längerem Gebrauch ausgewechselt werden müssen. Deswegen wird der Schlüsselbehälter aus einer Oberschale und aus einer Unterschale gebildet, die bedarfsweise voneinander gelöst werden müssen. Die Zerlegung und der Zusammenbau der Schalteile sind schwierig und zeitaufwendig. Um den Flachs Schlüssel in der Ruhelage im Behälterinneren versteckt anzuordnen, ist eine seitliche Ausnehmung im Schlüsselbehälter vorgesehen, aus welcher der mechanische Flachs Schlüssel in seiner Gebrauchslage herausfährt. Durch die Fuge zwischen der Ober- und Unterschale können Schmutz und Feuchtigkeit ins Behälterinnere gelangen, weshalb es dort auf eine gute Dichtung ankommt. Diese Abdichtung ist aber nach längerer Gebrauchsdauer nicht immer gewährleistet, zumal wenn elektronische Bauteile oder Batterien ausgetauscht werden. Der Ausbau und das Einbringen der elektronischen Bauteile und der Batterien im Gehäuseinneren ist mühsam und zeitaufwendig. Bei der Zerlegung und dem Zusammenbau des Schlüsselbehälters mit seinen beiden Schalen besteht die Gefahr, dass die Dichtung nicht mehr ordnungsgemäß plaziert bzw. dabei beschädigt wird. Eine ähnliche Lösung mit den gleichen Nachteilen beschreibt die EP 0 267 429 A1.

Des Weiteren ist aus der GB 2 080 386 A bekannt, einen mechanischen Schlüssel mit einer aufsteckbaren Kassette zu versehen. Die aus zwei Schalen bestehende Kassette, die eine Lichtquelle enthält, bildet eine gehäuseartige Kapsel und kann als Steckeinheit nachträglich eingesteckt oder festgelegt werden. Der Schlüsselgriff besitzt dazu eine Ausnehmung, welche einen von außen zugänglichen Freiraum bildet. Nachteilig bei dieser Anordnung ist, dass die Steckeinheit in Einsteckposition nicht gesichert ist und sich einfach aus der Steckverbindung lösen kann.

Der Erfindung liegt die Aufgabe zugrunde, einen zuverlässigen, raumsparenden Schlüssel der im Oberbegriff des Anspruches 1 genannten Art zu entwickeln, bei dem es keine Dichtungsprobleme gibt und bei dem der Austausch von elektronischen Bauteilen und gegebenenfalls Batterien unproblematisch sind. Dies wird erfindungsgemäß durch die im Kennzeichen von Anspruch 1 erwähnten Maßnahmen erreicht, denen folgende besondere Bedeutung zukommt.

Die Erfindung braucht sich mit dem Dichtungsproblem zwischen der Ober- und Unterschale des Schlüsselbehälters nicht zu befassen, weil die auf Schmutz und Feuchtigkeit sehr empfindlichen elektronischen Bauteile, zu denen gegebenenfalls elektrische Batterien gehören, von einer gehäuseartigen Kapsel umschlossen sind, mit der sie eine vorgefertigte Baueinheit bildet, die nachfolgend kurz „Elektrokapsel“ bezeichnet werden soll. Die in der Elektrokapsel befindlichen Elemente sind allseitig versiegelt. Bedarfsweise können die elektronischen Bauteile in der Elektrokapsel eingegossen sein. Diese Elektrokapsel ist dichtungsmäßig autark und bringt daher keine Dichtungsprobleme im Schlüsselbehälter. Die elektronischen Bauteile und ihre elektrischen Batterien sind im Inneren der Elektrokapsel nach außen geschützt untergebracht. Die Elektrokapsel wird ohne den zweischaligen Schlüsselbehälter zerlegen zu müssen, schnell und bequem in den Freiraum des Schlüsselbehälters eingesteckt und wieder entnommen werden. Die Elektrokapsel kann als eigenständiges Handelsprodukt in Verkehr gebracht werden, der vom Besitzer des Schlüssels erworben und mit dem stets geschlossen bleibenden Schlüsselbehälter zusammengesteckt werden kann.

Sowohl der Schlüsselbehälter mit seinem Ausbruch einerseits als auch die Elektrokapsel andererseits werden für sich vorgefertigt und sind jederzeit miteinander montierbar bzw. voneinander demontierbar. Weil der Schlüsselbehälter nicht in seine beiden Schalen zerlegt zu werden braucht, treten dort keine Dichtungsprobleme auf. Im übrigen ist es unmaßgeblich, ob bei eingesteckter Elektrokapsel der Schlüsselbehälter abgedichtet ist, denn dort

befinden sich nur die hinsichtlich Schmutz und Feuchtigkeit unempfindlichen Bauteile, wie der mechanische Flachs Schlüssel. Der Ausbruch im Schlüsselbehälter wird von der eingesteckten Elektrokapsel verschlossen. Die Elektrokapsel vervollständigt den Schlüsselbehälter zu einem bei der Schlüsselbetätigung gemeinsam zu handhabenden Kombinationsgehäuse. Die zur Handhabung dienende Fläche des Kombinationsgehäuses wird also teils vom Schlüsselbehälter des mechanischen Flachs Schlüssels und teils von der freibleibenden Umfangsfläche der Elektrokapsel gebildet. An den Übergangsstellen wird man für einen bündigen Übergang sorgen.

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 schematisch dargestellt. Es zeigen:

- Fig. 1, in perspektivischer Darstellung, den Schlüsselbehälter mit herausragendem mechanischen Flachs Schlüssel,
- Fig. 2, ebenfalls in perspektivischer Darstellung, eine zum Flachs Schlüssel von Fig. 1 gehörende Steckeinheit, bestehend aus einer die elektronischen Bauteile umschließenden Elektrokapsel,
- Fig. 3 ein aus dem Schlüsselbehälter von Fig. 1 und der Steckeinheit von Fig. 2 zusammengestecktes Kombinationsgehäuse, das zur Handhabung bei mechanischer und elektronischer Betätigung des Schlüssels dient,
- Fig. 4, in Explosionsdarstellung, einige wesentliche Bestandteile des in Fig. 1 gezeigten Schlüsselbehälters mit dem mechanischen Flachs Schlüssel, vor deren Zusammenbau,

- Fig. 5, in Explosionsdarstellung, die beiden Bestandteile des mechanischen Flachschlüssels vor ihrer Vereinigung,
- Fig. 6 einen Querschnitt durch den einen Bestandteil von Fig. 5, längs der dortigen Schnittlinie VI - VI,
- Fig. 7 einen Querschnitt durch das zusammengebaute Schlüsselbehälter von Fig. 1 längs der dortigen Schnittlinie VII - VII, wobei ein Druckknopf in seiner eingedrückten Position gezeigt ist,
- Fig. 8 einen Axialschnitt durch den in Fig. 1 gezeigten Schlüsselbehälter längs der dortigen Schnittlinie VIII - VIII und
- Fig. 9 einen Querschnitt durch das in Fig. 3 gezeigte Kombinationsgehäuse längs der dortigen Schnittlinie IX - IX.

Der kombinierte Schlüssel nach der Erfindung erlaubt sowohl eine mechanische als auch eine elektronische Betätigung eines nicht näher gezeigten Schlosses. Er besteht aus zwei jeweils für sich vorgefertigten Teilen 10, 20, die nachträglich ineinandergefügt werden. Der eine Teil 10 umfasst die mechanischen Schließmittel und besteht aus einem Schlüsselbehälter 10, dessen Bestandteile aus der Explosionsdarstellung von Fig. 4 am besten zu erkennen sind. Der andere Teil 20 ist eine noch näher zu beschreibende Steckeinheit, welche die in ihrem Inneren die im Querschnitt von Fig. 9 angedeuteten elektronischen Bauteile 40 umfasst.

Ausweislich der Fig. 1 und 4 umfasst der mechanische Teil zunächst einen zweisehaligen Schlüsselbehälter 10. Während die Oberschale 11, wie Fig. 7 und 8 erkennen lässt, als ebene Platte mit stellenweisen Kupplungsvorsprüngen 13 an



ihrer Innenfläche ausgebildet ist, umfasst die Unterschale 12 außer ihrem Schalenboden 15 auch noch Schalenseitenwände 14. In den Schalenseitenwänden 14 befinden sich stellenweise Kupplungsaufnahmen 16 für die vorerwähnten Kupplungsvorsprünge 13 der Oberschale 11. Die Oberschale 11 erstreckt sich nur über einen vorderen Bereich des Schlüsselbehälters 10 und weist im hinteren Bereich einen Ausbruch 17 auf, der zum Schaleninneren 18 hin einen von außen zugänglichen Freiraum erzeugt. Das ist für das noch näher zu beschreibende Einstecken bzw. Herausziehen der Steckeinheit 20 bedeutungsvoll.

Zum Schlüsselbehälter 10 gehört, wie Fig. 4 zeigt, ein mechanischer Flachs Schlüssel 30 der beweglich angeordnet ist, um aus einer nicht näher gezeigten versenkten Ruhelage im Behälter 10 in eine aus dem Behälter herausragenden, in Fig. 1 bis 4 ersichtliche Gebrauchslage überführt zu werden. Der Flachs Schlüssel 30 besteht aus metallischem Werkstoff. Obwohl auch andere Bewegungen denkbar wären, ist dieser Flachs Schlüssel 30 um die strichpunktiert in den Fig. 1, 3 und 4 angedeuteten Schwenkachsen 33 schwenkbeweglich. Dabei ist der Flachs Schlüssel 30 als ein Stanzling aus einer in Fig. 4 strichpunktiert verdeutlichten ebenen Platte 34 ausgebildet, wobei der Stanzling ein L-förmiges Umrissprofil aus zwei Schenkeln 31, 32 besitzt. Der eine L-Schenkel ist kurz ausgebildet und dient zur Schwenklagerung des Flachs Schlüssels 30 am Vorderende des Schlüsselbehälters 10 und wird daher nachfolgend kurz „Lagerschenkel“ genannt. Der andere L-Schenkel 32 umfasst das eigentliche Flachprofil des Schlüsselschafts, weshalb er nachfolgend als „Schaftschenkel“ bezeichnet werden soll. Beide Schenkel 31, 32 liegen also in einer gemeinsamen, durch den erwähnten Plattenverlauf 34 bestimmten Ebene, die im fertig montierten Zustand des Schlüsselbehälters 10 senkrecht zur Schwenkachse 33 verläuft. Ausweislich der Fig. 5 ist der Lagerschenkel 31 mit einem unrundern Plattendurchbruch 35 versehen, der zur Aufnahme eines besonderen Einsatzes 36 dient.

Der Druckknopf 40 ist sowohl axial als auch radial federbelastet und besitzt mit dem Behälter 10 übereinstimmend ausgebildete Profile 19, 48, 28. Der Einsatz 36

besteht aus relativ nachgiebigem Material, vorzugsweise Kunststoff und besitzt ein besonderes Gegenprofil 37, 38, 39 für einen die Lage der Schwenkachse 33 bestimmenden Druckknopf 40. Die Federwirkung übernimmt eine kombinierte Druck-Dreh-Feder 41, die, ausweislich der Fig. 7, in einer Axialbohrung 45 des Druckknopfs 40 aufgenommen ist. Die Feder 41 ist mit ihrem einen Federende 42 drehfest mit dem Druckknopf 40 verbunden, während ihr anderes Federende 43 in der Unterschale 12 des Behälters 10 festgehalten wird. Die Feder 41 ist wendelförmig ausgebildet. Im Montagefall greift ein an der bodenseitigen Innenfläche der Unterschale 12 sitzender Dorn 44 sowohl ins Wendelinnere hinein, als auch in den Einsatz 36 ein.

Gemäß Fig. 5 wird zunächst der Flachs Schlüssel 30 mit seinem Plattendurchbruch 35 durch Stanzen erzeugt und dann, nachträglich, der Einsatz 36 in den Plattendurchbruch 35 vertikal eingesteckt. Nach diesem Einstecken ragt, wie Fig. 4 und 7 zeigen, über die beiden Plattenflächen des Flachs Schlüssels heraus. Dazu gehören zylindrische Ansätze 47, gemäß Fig. 6, aber auch ein Anschlagzapfen 39 an beiden Flächenseiten, der in ein Ringnutsegment 19 der beiden Schalen 11 und 12 hineinragt, wie aus Fig. 8 zu entnehmen ist. In der in Fig. 8 ausgezogen gezeichneten Position des Anschlagnockens 39 liegt die bereits eingangs erwähnte, aus dem Behälter 10 herausgeschwenkte Gebrauchslage vor. Dann erstreckt sich der vorbeschriebene Schaftschenkel 32 des Flachs Schlüssels 30 in Richtung der in Fig. 8 strichpunktiert angedeuteten Hilfslinie 30.1, welche die in den übrigen Fig. dargestellte Gebrauchslage des Flachs Schlüssels 30 kennzeichnet. In dieser Gebrauchslage 30.1 ist der Flachs Schlüssel durch den Druckknopf 40 arretiert. Dann greifen am Druckknopf 40 vorgesehene, hier diametral angeordnete Mitnahme flügel 48 in zugehörige Radialnuten 28 an der Innenfläche der Oberschale 11 hinein und sichern so die Ausschwenklage des Flachs Schlüssels 30.

Die Mitnahme flügel 48 besitzen, als Gegenprofil, im Einsatz 36 Axialnuten 48, die eine Eindruckbewegung im Sinne des aus Fig. 7 erkennbaren Kraftpfeils 46 zulassen. Diese Eindruckbewegung 46, die in Fig. 7 vollzogen ist, führt zu einer

axialen Absenkung des Druckknopfs 40, wodurch die Mitnahmeflügel 48 die Radialnuten 28 freigeben. Die Eindruckbewegung 46 erfolgt gegen die axiale Kraftwirkung der Feder 41. Die Arretierung der Gebrauchslage 30.1 ist dann aufgehoben. Der Flachschlüssel kann dann im Sinne des Bewegungspfeils 29 von Fig. 8 gegen die durch den Kraftpfeil 49 in Fig. 8 verdeutlichte Drehkraft der Feder 41 in seine Ruhelage im Gehäuse zurückgeschwenkt werden. Dann liegt der Schaftschenkel 32 des Flachschlüssels 30, in Fig. 8 gesehen, an der dort mit 30.2 gekennzeichneten Strichpunktlinie. In dieser Ruhelage 30.2 verschwindet der Schaftschenkel 32 in einem aus Fig. 3 erkennbaren seitlichen Spalt 24 eines noch näher zu beschreibenden Gesamtgehäuses 50, welches aus dem Schlüsselbehälter 10 und der darin eingeschobenen Steckeinheit 20 entsteht. Dann sind die Mitnahmeflügel 48 wieder in axialer Ausrichtung mit den gehäuseseitigen Radialnuten 28, wo sie durch die Rückstellkraft der Feder 41 einschnappen und so auch diese Ruhelage 30.2 des Flachschlüssels 30 im Schlüsselbehälter 10 arretieren.

Bei der Schwenkbewegung 29 dient der Druckknopf 40 auch als Schwenklager. Dazu ist in der Oberschale 11 des Behälters 10 eine aus Fig. 4 erkennbare Lagerbohrung 25 vorgesehen. Diese ist in axialer Ausrichtung mit einer in Fig. 5 und 6 gezeigten Axialbohrung 37 des Einsatzes 36 und mit dem bereits mehrfach erwähnten Dorn 44 der Unterschale 12. Der Druckknopf 40 bestimmt die Schwenkachse 33 des Flachschlüssels 30. Der Anschlagzapfen 39 vom Einsatz 36 einerseits und das ihm gehäuseseitig zugeordnete Ringnutsegment 19 andererseits können auch Drehführungsfunktionen bei der Schwenkbewegung 29 übernehmen. Außerdem können Drehanschläge durch das Umrissprofil des Schlüssels 30 einerseits und Innenflächen an den beiden Schalen 11, 12 andererseits verwirklicht sein.

Statt einer Vorfertigung des Einsatzes 36 könnte man den Einsatz 36 durch eine Spritzgusstechnik nachfertigen. Dazu wird der beschriebene Flachschlüssel 30 in eine Spritzgussform eingebracht, in welcher dann der Einsatz 36 im

Plattendurchbruch 35 durch Gießen gebildet wird. Die erwähnte Gegenprofilierung 37, 38, 39, 47 liegt dann in ähnlicher Form vor.

In manchen Anwendungsfällen ist bei dem eingangs erwähnten kombinierten Schlüssel für die elektronische Betätigung auch ein sogenannter Transponder 26 erwünscht. Dieser Transponder 26 soll bereits zur elektronischen Individualisierung dieses kombinierten Schlüssels sorgen. Wird dieser Schlüssel in das zugehörige Schloss eingesteckt, so findet zwischen dem Transponder 26 und dem Schloss eine Kommunikation statt, die bei Übereinstimmung von Schloss und Schlüssel bereits Schlossfunktionen auslöst. Deswegen werden bei der Erfindung derartige Transponder 26 im vorderen Bereich des Schlüsselbehälters 10 untergebracht. Dazu besitzt die Unterschale 12 eine Kammer 27, in welche der bzw. die Transponder 26 eingeklebt werden können. Weil eine elektronische Energieversorgung der Transponder 26 nicht erforderlich ist, braucht der fertig montierte Schlüsselbehälter 10 von Fig. 1 nicht mehr in seine Schalen 11, 12 zerlegt zu werden, um dort einen Batteriewechsel od. dgl. vorzunehmen. Die Transponder 26 sind also in der Kammer 27 permanent geschützt. Das gilt auch für die bereits eingangs erwähnten weiteren elektronischen Bauteile 21, welche innerer Bestandteil der bereits erwähnten lösbaren Steckeinheit 20 des Gesamtgehäuses 50 sind.

Wie am besten aus Fig. 9 zu ersehen ist, gehören zur Steckeinheit 20 eine gehäuseartige Kapsel 22, in deren Innenraum 23 die Bauteile 21 angeordnet und so nach außen allseitig abgeschlossen sind. Im Kapselinneren 23 können auch die Schaltungen der Bauelemente und gegebenenfalls die elektrische Störung angeordnet sein. Diese Baueinheit 21, 22, die als Steckeinheit mit dem Schlüsselbehälter 10 fungiert, wird komplett vorgefertigt und soll nachfolgend „Elektrokapsel“ genannt werden. Dazu ist der Schlüsselbehälter 10 profilmäßig in folgender Weise angepasst.

Der eingangs erwähnte Ausbruch 17 im Schlüsselbehälter 10 erfolgt einfach dadurch, dass die Oberschale 11, gemäß Fig. 1, nur den Vorderabschnitt 51 des Schlüsselbehälters 10 überdeckt. Dadurch ist ein von außen zugänglicher Freiraum ins Schaleninnere 18 erzeugt. Dieser Freiraum 17 besitzt nicht nur eine nach oben weisende Oberöffnung 52, sondern erstreckt sich auch in eine vom Hinterende 54 zugängliche Seitenöffnung 53. Diese entsteht, weil nicht nur der hintere Abschnitt der Oberschale 11 fehlt, sondern auch, wie Fig. 1 zeigt, die Seitenwand 14 der Unterschale 12 am Hinterende 54 des Behälters 10 weggefallen ist. Die Elektrokapsel 20 wird durch diese Seitenöffnung 53 in den Freiraum 17 des Schlüsselbehälters 10 gemäß dem Bewegungspfeil 55 von Fig. 1 eingeschoben. In ihrer Einschublage, gemäß Fig. 3, verschließt die Elektrokapsel 20 die Oberöffnung 52. Die Einschubbewegung 55 ist in einer Parallelebene zu der oben erwähnten Schwenkbewegung 29 angeordnet. Dabei sind folgende Führungsmittel 61, 62 zum gezielten Einstecken und Verschieben 55 der Elektrokapsel 20 vorgesehen.

An der Innenfläche des Schalenbodens 15 der Unterschale 12 befinden sich zwei parallele Führungsleisten 61, die zur Seitenöffnung 53 hin gerichtet sind. Sie sind hinterschnitten und besitzen vorzugsweise ein schwalbenschwanzförmiges Profil. Ihnen sind angepasste Führungsnuten 62 an der Unterseite des Gehäuses der Elektrokapsel 20 zugeordnet. Die Eingriffslage dieser Führungsmittel 61, 62 ist im Schnitt von Fig. 9 zu erkennen. Dabei ist die eine Längsseite vom Kapselgehäuse 22 gemäß Fig. 9 bei 58 gestuft, so dass mit einer entsprechenden Stufung 59 in der Unterschale 12, gemäß Fig. 4, in der Einschublage der seitliche Spalt 24 für den Schaftschenkel 32 des Flachschlüssels 30 entsteht. In der Einschublage gemäß Fig. 3 und 9 gehen die sichtbar bleibenden Außenflächen der Elektrokapsel 20 einerseits und des Schlüsselbehälters 10 andererseits ineinander bündig über. Beide Teile 10, 20 bilden dann das bereits erwähnte Kombinationsgehäuse 50, welches beim Handhaben des Schlüssels mit der Hand gemeinsam umgriffen wird und daher „Kombinationsgehäuse“ genannt werden soll. Dies gilt sowohl bei einer mechanischen Betätigung des zugehörigen Schlosses, wo der herausgeschwenkte

Schaftschenkel 32 mittels des Kombigehäuses 50 gedreht wird, als auch bei der elektronischen Betätigung. Dafür sind Betätigungsstellen 60 an die sichtbar bleibende Außenfläche der Elektrokapsel 20 im gemeinsamen Kombinationsgehäuse 50 vorgesehen. Diese können aus Druckschaltern oder membranartigen Betätigungsstellen entstehen. Diese Betätigungsstellen können mit weiteren membranartigen Überdeckungen im Bereich des vorerwähnten Druckknopfs 40 vorgesehen sein, dem noch folgende besondere Bedeutung zukommt.

Die in Fig. 3 und 9 gezeigte Einstecklage der Elektrokapsel 20 im Schlüsselbehälter 10 ist nicht nur durch Anschlagmittel begrenzt, sondern auch durch Rastmittel gesichert. Diese Funktion kann in vorteilhafterweise auch vom Druckknopf 40 übernommen werden. Dazu ist die Elektrokapsel 20, gemäß Fig. 2, vorderendig mit einem Lappen 56 verlängert, der in der Einschublage von Fig. 3 den verbliebenen Vorderabschnitt 51 der Oberschale 11 vom Schlüsselbehälter 10 überdeckt. Der Lappen 56 besitzt eine Ausnehmung 57, in welche der axial federnde Druckknopf 40 in der Einschublage der Elektrokapsel 20 gemäß Fig. 3 einschnappt. Dadurch ist der Zusammenhalt des Schlüsselbehälters mit der Elektrokapsel 20 sichergestellt. Die Ausnehmung 57 durchsetzt den Lappen 56, weshalb im Eingriffsfall gemäß Fig. 3 der Druckknopf 40 mit einem zu seiner Betätigung ausreichenden Längenstück aus dem Lappen 56 herausragt. Zur Demontage des Kombinationsgehäuses 50 in seine Bestandteile 10, 20 wird der Druckknopf 40, wie Fig. 7 zeigt, soweit im Sinne des Pfeils 46 eingedrückt, dass er die Ausnehmung 57 im Lappen 56 freigibt.

Der Druckknopf 40 kann durch eine Membran im Bereich des Lappens 56 überdeckt sein, welche in ähnlicher Weise wie die Betätigungsstellen 61 fungiert. Diese Membrane dieser Betätigungsstellen 61 können mit der vorgenannten Membran im Bereich des Druckknopfs 40 kombiniert sein.

## Bezugszeichenliste :

- 10 erster Schlüsselteil, Schlüsselbehälter
- 11 Oberschale von 10
- 12 Unterschale von 10
- 13 Kupplungsvorsprung an 11
- 14 Schalenseitenwand von 12
- 15 Schalenboden von 12
- 16 Kupplungsaufnahme von 12
- 17 Ausbruch von 11, Freiraum in 18
- 18 Schaleninneres
- 19 Profil in 11, 12 für 39, Ringnutsegment
- 20 zweiter Schlüsselteil, Steckeinheit, Elektrokapsel
- 21 elektronischer Bauteil
- 22 gehäuseartige Kapsel für 21
- 23 Kapselinneres für 22 in 21
- 24 seitlicher Spalt in 50 für 32 (Fig. 3, 9)
- 25 Lagerbohrung in 11 für 40 (Fig. 4)
- 26 Transponder
- 27 Kammer in 11 für 26 (Fig. 4)
- 28 Profil in 11 für 48 von 40, Radialnut (Fig. 7)
- 29 Schwenkbewegungspfeil für 30 (Fig. 8)
- 30 mechanischer Flachschlüssel für 10, Stanzling
- 30.1 Gebrauchslage von 32 (Fig. 8)
- 30.2 Ruhelage von 32 (Fig. 8)
- 31 erster L-Schenkel von 30, Lagerschenkel
- 32 zweiter L-Schenkel von 30, Schaftschenkel
- 33 Schwenkachse für 30
- 34 ebene Platte für 30
- 35 Plattendurchbruch

- 36 Einsatz in 35
- 37 Gegenprofil in 36, Axialbohrung (Fig. 5, 6)
- 38 Gegenprofil von 36, Axialnut in 36 für 48 (Fig. 5, 8)
- 39 Gegenprofil von 36, Führungs- bzw. Anschlagzapfen (Fig. 5, 6)
- 40 Druckknopf
- 41 Druck-Dreh-Feder von 40
- 42 erstes Federende von 41 (Fig. 7)
- 43 zweites Federende von 41 (Fig. 7)
- 44 Dorn an 12 für 41 (Fig. 4)
- 45 Axialbohrung in 40 für 41
- 46 Pfeil der Eindruckbewegung von 40 (Fig. 7)
- 47 Gegenprofil an 36, zylindrischer Ansatz an 36 (Fig. 5)
- 48 Profil, Mitnahmevlügel an 40
- 49 Pfeil der Ausschwenkkraft von 41 für 30 (Fig. 8)
- 50 Gesamtgehäuse aus 10, 20, Kombinationsgehäuse
- 51 Vorderabschnitt von 10
- 52 Oberöffnung von 10 bei 17 (Fig. 1)
- 53 Seitenöffnung von 11 (Fig. 1)
- 54 Hinterende von 10
- 55 Pfeil der Einschubbewegung von 20 in 10 (Fig. 1)
- 56 Lappen an 20 (Fig. 2)
- 57 Ausnehmung in 56 für 40 (Fig. 2)
- 58 Innenstufung von 22 für 24 (Fig. 2, 9)
- 59 Stufe von 12 für 24 (Fig. 4)
- 60 Betätigungsstelle an 20 (Fig. 1)
- 61 Führungsmittel an 12, Führungsleiste
- 62 Führungsmittel an 20, Führungsnut



P a t e n t a n s p r ü c h e :

- 1.) Kombiniertes mechanisches und elektronisches Schlüssel, insbesondere für in Fahrzeugen befindliche Schlösser,

mit einem gemeinsamen, bei der Schlüsselbetätigung zu handhabenden Schlüsselbehälter (10) sowohl für elektronische Bauteile (21) zur elektronischen Betätigung als auch für einen Flachslüssel (30) zur mechanischen Betätigung des Schlosses,

wobei der Flachslüssel (30) im Behälter beweglich (29) aufgenommen ist und aus einer im Behälter (10) versenkten Ruhelage (30.2) in eine aus dem Behälter (10) herausragende Gebrauchslage (30.1) überführbar ist,

und mit einem im Behälter (10) angeordneten axial gefederten (41) Druckknopf (40), der den Schlüssel (30) in wenigstens einer dieser Lagen (30.1; 30.2) arretiert,

wobei der Schlüsselbehälter (10) aus einer Ober- und Unterschale (11, 12) besteht, die wenigstens bereichsweise aneinander befestigt sind,

d a d u r c h g e k e n n z e i c h n e t ,

daß die Oberschale (11) in ihrem außerhalb des Druckknopfs (40) liegenden Bereich einen Ausbruch (17) aufweist,

daß der Ausbruch einen von außen zugänglichen Freiraum (17) im Schaleninneren (18) erzeugt,

daß die elektronischen Bauteile (21), deren Schaltung und gegebenenfalls elektrische Steuerung von einer gehäuseartigen Kapsel (22) umschlossen sind und mit dieser eine vorgefertigte

daß die Elektrokapsel (20) eine Steckeinheit bildet, welche nachträglich in den Freiraum (17) des fertig montierten Schlüsselbehälters (10) einsteckbar (55) und dort festlegbar ist,

daß die Elektrokapsel (20) einen sie vorderendig verlängerten Lappen (56) besitzt,

daß in der Einschublage der Kapsel (20) der Lappen (56) das vor der Oberöffnung (52) des Schlüsselbehälters befindliche Raststück (51) der Oberschale (11) wenigstens bereichsweise überdeckt,

und daß der Lappen (56) eine Ausnehmung (57) aufweist, in welcher der federnde (41) Druckknopf (40) axial einfährt und die Einschublage der Elektrokapsel (20) im Schlüsselbehälter (10) sichert.

- 2.) Schlüssel nach Anspruch 1, dadurch gekennzeichnet, dass die eingesteckte Elektrokapsel (20) auf ihrer im Ausbruch (17) freiliegenden Flächenbereichen Betätigungsstellen (60) zum Wirksamsetzen der in ihrem Inneren befindlichen elektronischen Bauteile (21) besitzt.

- 3.) Schlüssel nach Anspruch 1 oder 2, dadurch gekennzeichnet, dass die eingesteckte Elektrokapsel (20) den Ausbruch (17) im Schlüsselbehälter (10) verschließt

und dass die Steckkombination aus der Elektrokapsel (20) einerseits und dem Schlüsselbehälter (20) andererseits ein Kombinationsgehäuse (50) mit bündig übergewandter Umfangsfläche erzeugt.

- 4.) Schlüssel nach einem oder mehreren der Ansprüche 1 bis 3, dadurch gekennzeichnet, dass der Ausbruch (17) nicht nur eine nach oben weisende Oberöffnung (52) erzeugt, die durch Wegfall des hinteren Oberschalen-Abschnitts entsteht, sondern sich auch über eine Seitenöffnung (53) erstreckt, die durch einen wenigstens bereichsweisen Wegfall der Seitenwand (14) in der Unterschale (12) und gegebenenfalls in der Oberschale (11) entsteht,

dass die Elektrokapsel (20) durch die Seitenöffnung (53) in den Freiraum (17) des Schlüsselbehälters (10) einschiebbar (55) ist und in ihrer Einschublage auch die Oberöffnung (52) wenigstens bereichsweise verschließt.

- 5.) Schlüssel nach einem oder mehreren der Ansprüche 1 bis 4, wobei der Flachschlüssel (30) zwischen seiner Ruhe- und Gebrauchslage (30.2; 30.1) im Behälter (10) verschwenkbar (29) ist,

wobei der Druckknopf (40) als Schwenklager (33) für den Flachschlüssel (30) dient und seine Federung (41) bestrebt (49) ist, den Flachschlüssel (30) in dessen Gebrauchslage (30.1) herauszuschwenken,

d a d u r c h g e k e n n z e i c h n e t ,

dass die Einschubrichtung (55) der Elektrokapsel (50) in den Schlüsselbehälter (10) in einer Parallelebene zur Schwenkbewegung (29) des Flachschlüssels (30) angeordnet ist.

6.) Schlüssel nach Anspruch 4 oder 5, dadurch gekennzeichnet, dass die zum Einschub (55) der Elektrokapsel (20) dienende Seitenöffnung (53) sich an dem bezüglich des Druckknopfs (40) gegenüberliegenden Hinterende (54) des Schlüsselbehälters (10) befindet.

7.) Schlüssel nach einem oder mehreren der Ansprüche 4 bis 6, dadurch gekennzeichnet, dass die Unterschale (12) und die Elektrokapsel (20) Führungsmittel (61, 62) zum gezielten Einstecken und Verschieben (55) der Elektrokapsel (20) besitzen

und dass die Führungsmittel (61, 62) zur Seitenöffnung (53) der Unterschale (12) hin weisen.

8.) Schlüssel nach Anspruch 7, dadurch gekennzeichnet, dass die Führungsmittel (61, 62) in der Unterschale (12) zur Oberöffnung (52) des Schlüsselbehälters (10) hin hinterschnitten sind.

9.) Schlüssel nach Anspruch 7 oder 8, dadurch gekennzeichnet, dass die Führungsmittel aus mindestens einer, vorzugsweise aber zwei Führungsleisten (61) bestehen, die ein schwalbenschwanzförmiges Profil besitzen,

und dass die Elektrokapsel (20) dazu angepasste Führungsnuten (62) besitzt.

10.) Schlüssel nach einem oder mehreren der Ansprüche 1 bis 9, dadurch gekennzeichnet, dass die Einstecklage der Elektrokapsel (20) im Schlüsselbehälter (10) durch Anschlagmittel begrenzt und durch Rastmittel gesichert ist.

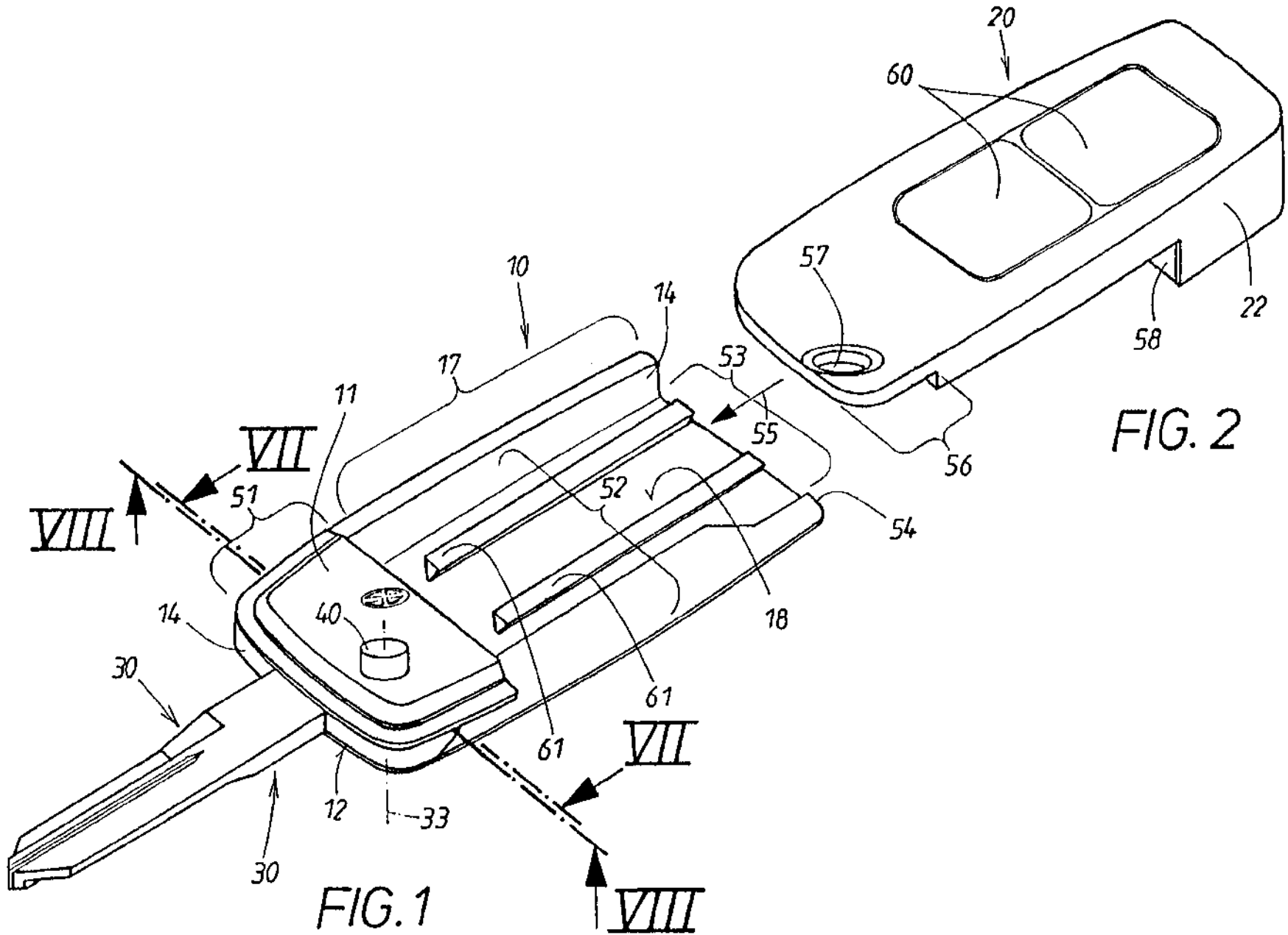
11.) Schlüssel nach Anspruch 11, dadurch gekennzeichnet, dass die Ausnehmung (57) den Lappen (56) durchsetzt

und dass der Druckknopf (40) in der Einschublage der Elektrokapsel (20) mit seinem Betätigungsende zu Betätigungszwecken aus der Lappenoberseite herausragt.

12.) Schlüssel nach Anspruch 11 oder 12, dadurch gekennzeichnet, dass am Druckknopf (40) und an seiner Aufnahme (44) im Schlüsselbehälter (10) Steuermittel (41, 48, 38, 37) angeordnet sind, die den Druckknopf (40) während der Schwenkbewegung (29) des Flachschlüssels (30) zwischen der Gebrauchs- und Ruhelage (30.1; 30.2) in einer axial eingedrückten Position halten,

und dass der Druckknopf (40) in dieser Eindrückposition aus der Ausnehmung (57) im Lappen (56) ausgefahren ist und die Elektrokapsel (20) freigibt.

- 13.) Schlüssel nach einem oder mehreren der Ansprüche 11 bis 13, dadurch gekennzeichnet, dass der Lappen (56) im Bereich seiner Ausnehmung (57) eine Membran aufweist, welche in Einschublage der Elektrokapsel (20) den Druckknopf (40) nach oben überdeckt,
- und dass diese Membran die manuelle Betätigungsstelle für den Druckknopf (40) bildet.
- 14.) Schlüssel nach Anspruch 13 oder 14, dadurch gekennzeichnet, dass die Membran mit dem Lappen (56) der Elektrokapsel (20) einstückig ausgebildet ist.
- 15.) Schlüssel nach Anspruch 14 oder 15, dadurch gekennzeichnet, dass die zur Betätigung des Druckknopfs (40) dienende Membran mit weiteren membranartigen Betätigungsstellen (60) im Schlüsselgehäuse (10) bzw. an der im Einsteckfall sichtbar bleibenden Außenfläche der Elektrokapsel (20) kombiniert ist, die zum Wirksamsetzen der elektronischen Bauteile (21) in der Elektrokapsel (20) dienen.



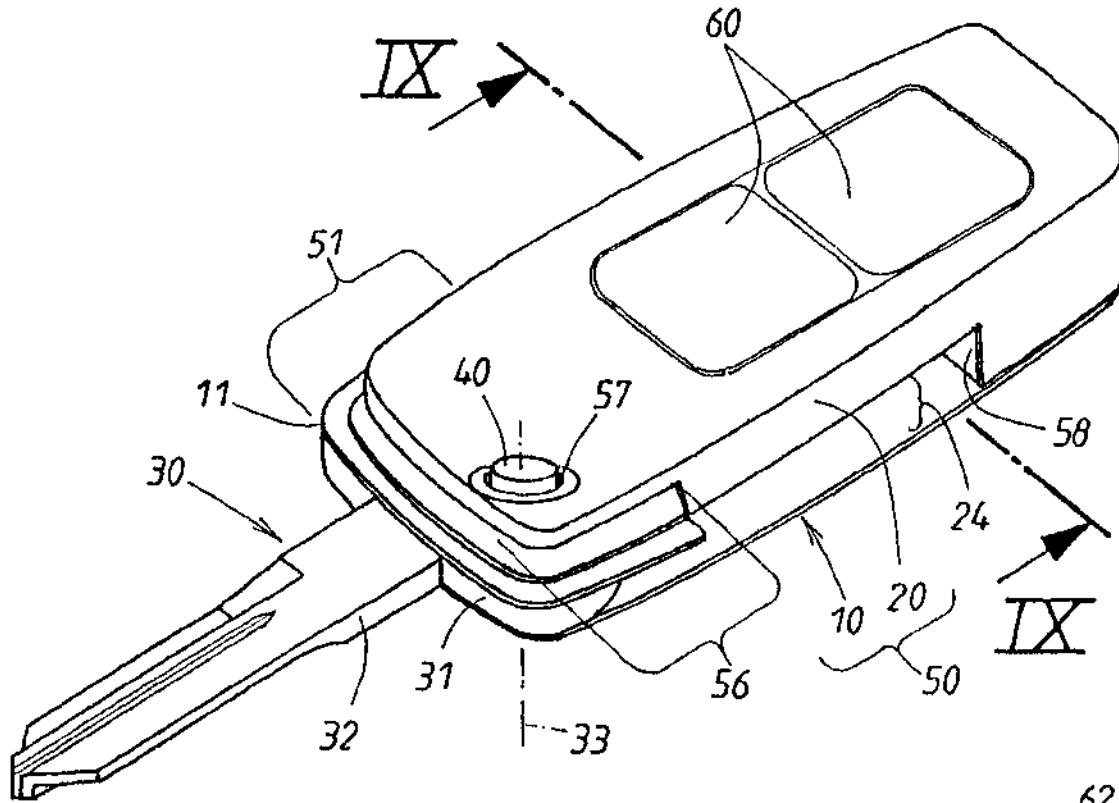


FIG. 3

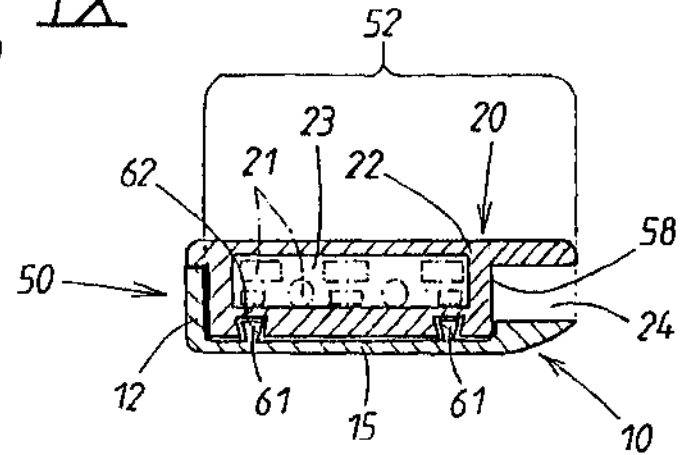


FIG. 9



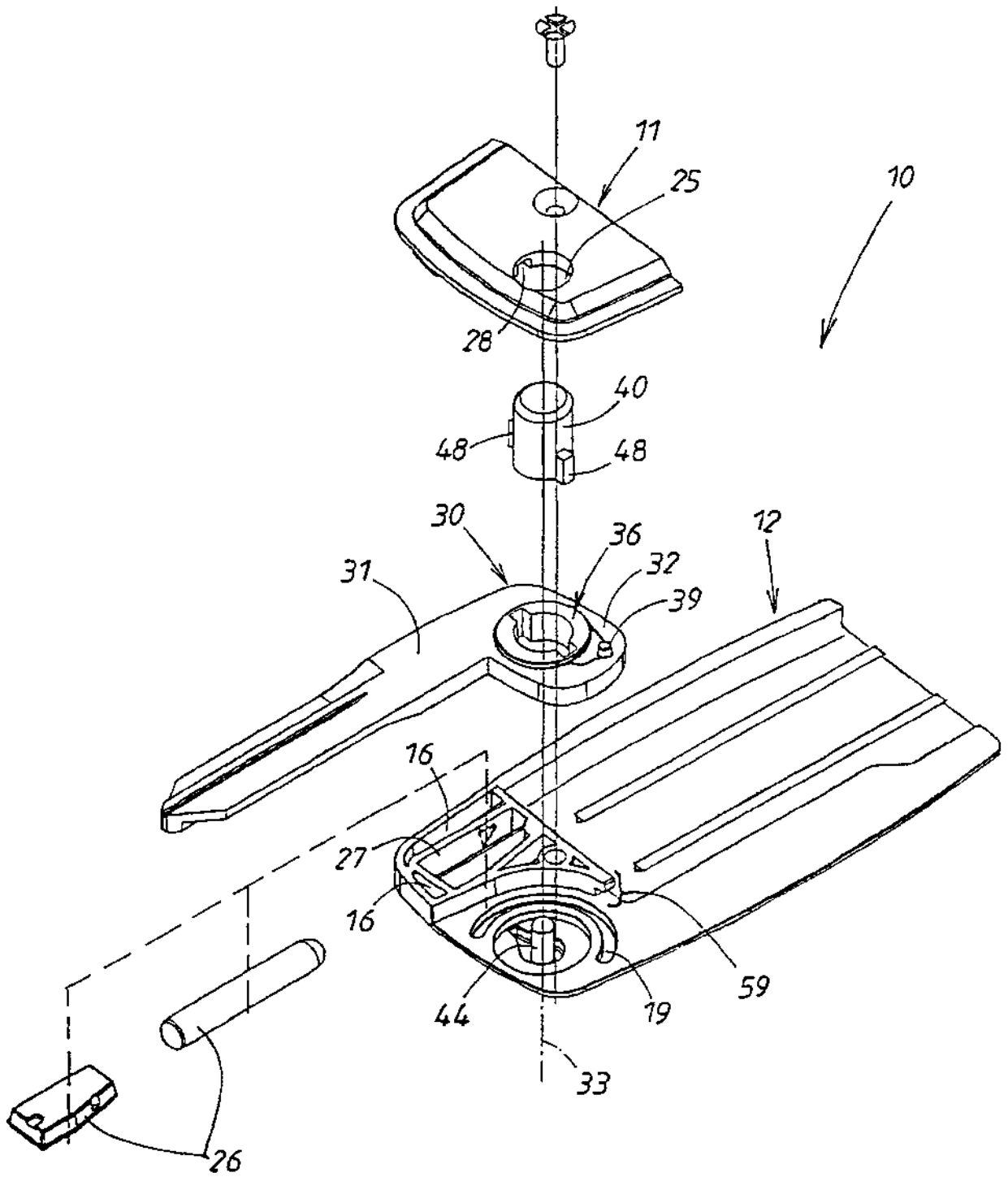
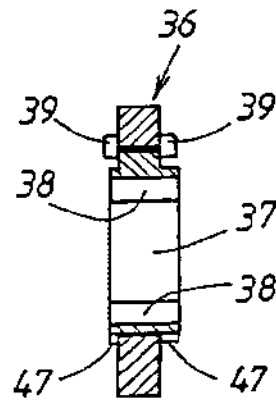
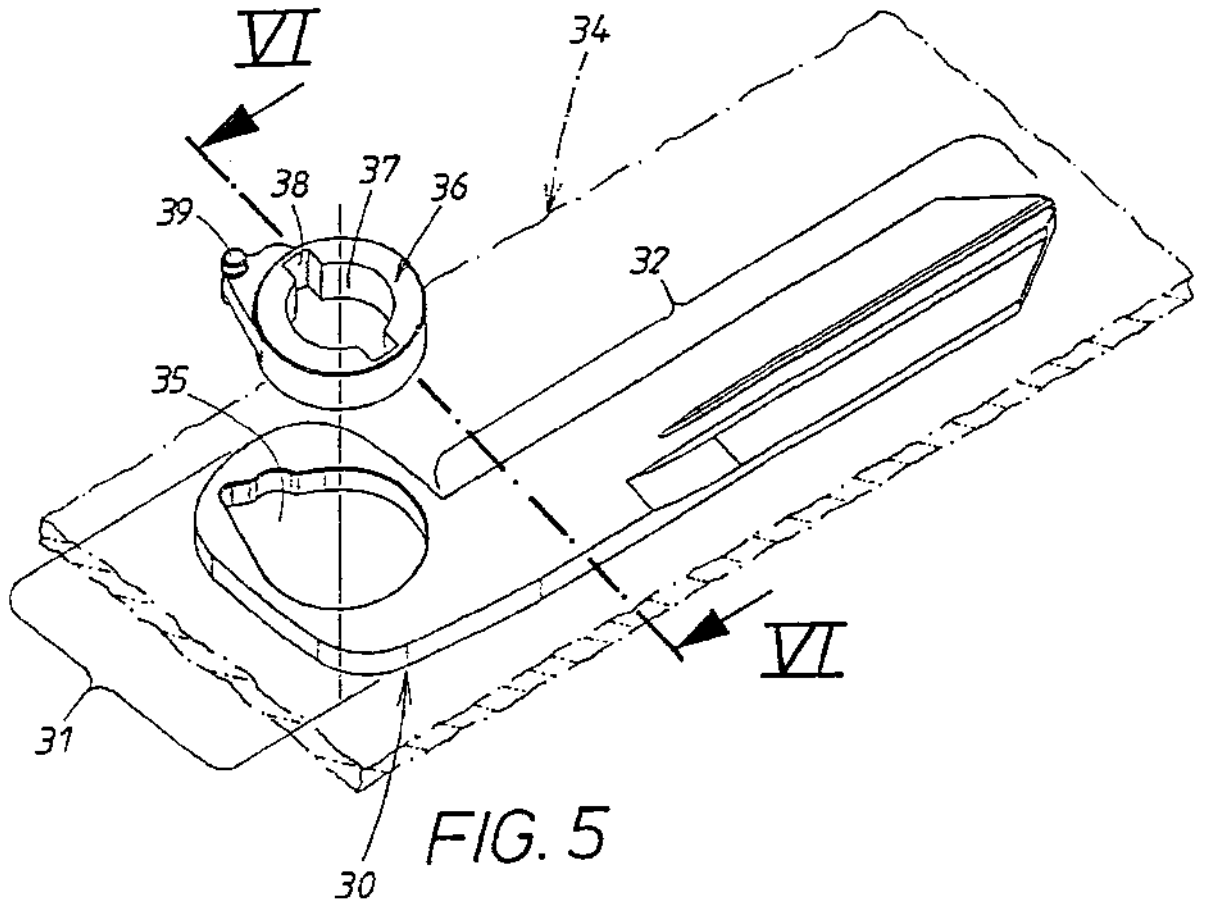


FIG. 4



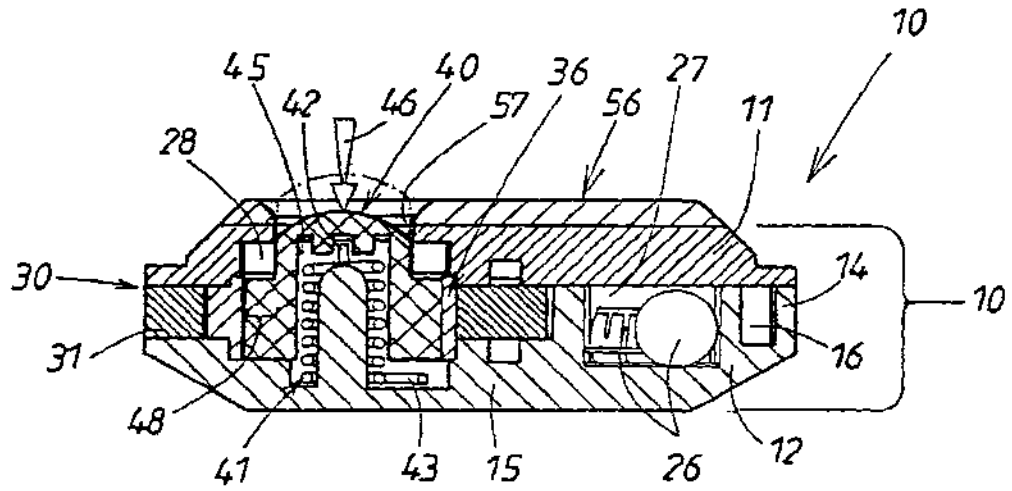


FIG. 7

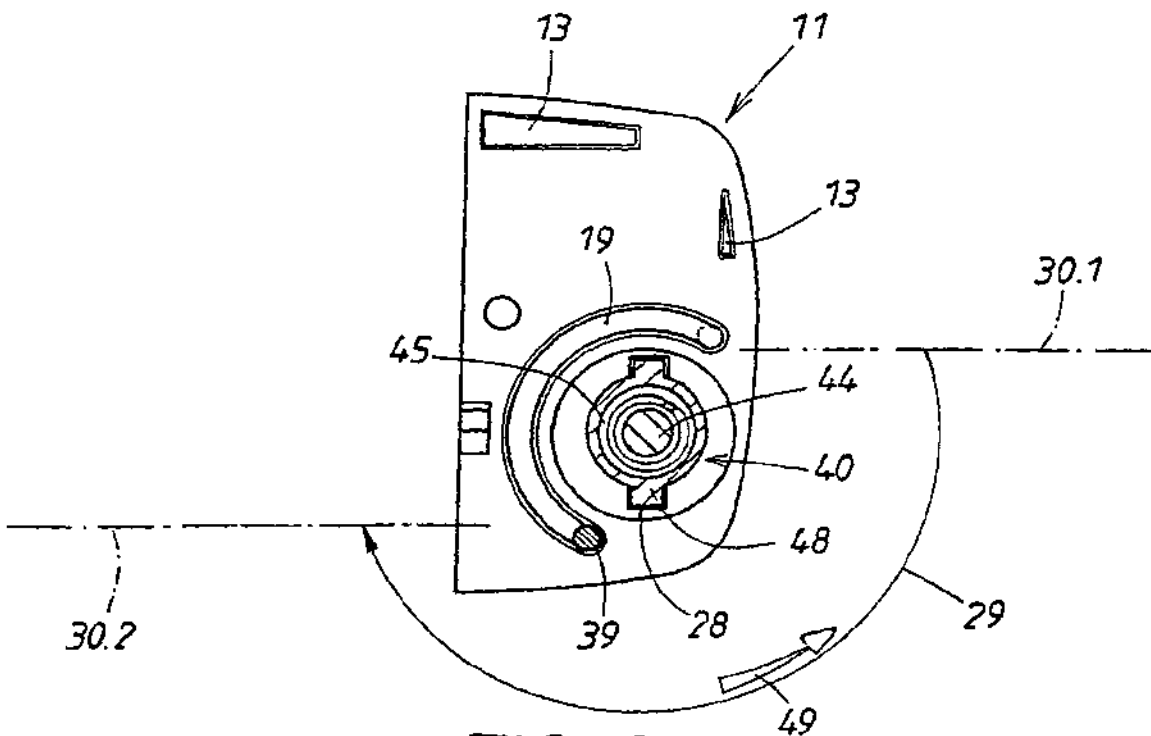


FIG. 8

# INTERNATIONAL SEARCH REPORT

Int. l. Application No  
PCT/EP 00/12431

**A. CLASSIFICATION OF SUBJECT MATTER**  
 IPC 7 E05B49/00 E05B19/00 E05B19/04

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 A45C

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used):  
 EPO-Internal

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	DE 39 02 537 A (DAIMLER BENZ AG ;HUELSBECK & FUERST (DE)) 9 August 1990 (1990-08-09) cited in the application the whole document	1
A	EP 0 267 429 A (SIEMENS AG) 18 May 1988 (1988-05-18) cited in the application the whole document	1
A	US 4 726 205 A (ALLERDIST HEINZ ET AL) 23 February 1988 (1988-02-23) column 1, line 31 - line 62 column 2, line 20 - line 38; figure	1

Further documents are listed in the continuation of box C.       Patent family members are listed in annex.

\* Special categories of cited documents:

<p>*A* document defining the general state of the art which is not considered to be of particular relevance</p> <p>*E* earlier document but published on or after the international filing date</p> <p>*L* document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)</p> <p>*O* document referring to an oral disclosure, use, exhibition or other means</p> <p>*P* document published prior to the international filing date but later than the priority date claimed</p>	<p>*T* later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention</p> <p>*X* document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone</p> <p>*Y* document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.</p> <p>*Z* document member of the same patent family</p>
--	--

Date of the actual completion of the international search  <b>16 March 2001</b>	Date of mailing of the international search report  <b>26/03/2001</b>
---	---

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  <b>Pieracci, A</b>
--	--

# INTERNATIONAL SEARCH REPORT

Information on patent family members

Int. l. Application No PCT/EP 00/12431
---

Patent document cited in search report	A	Publication date	Patent family member(s)	Publication date
DE 3902537	A	09-08-1990	NONE	
EP 0267429	A	18-05-1988	DE 3769923 D JP 63110377 A US 4888970 A	13-06-1991 14-05-1988 26-12-1989
US 4726205	A	23-02-1988	DE 3509579 A DE 3678983 D EP 0195195 A JP 61229079 A	18-09-1986 06-06-1991 24-09-1986 13-10-1986

# INTERNATIONALER RECHERCHENBERICHT

Internationales Aktenzeichen

PCT/EP 00/12431

**A. KLASSIFIZIERUNG DES ANMELDUNGSGEGENSTANDES**  
 IPK 7 E05B49/00 E05B19/00 E05B19/04

Nach der Internationalen Patentklassifikation (IPK) oder nach der nationalen Klassifikation und der IPK

**B. RECHERCHIERTE GEBIETE**

Recherchierter Mindestprüfstoff (Klassifikationssystem und Klassifikationssymbole)

IPK 7 E05B A45C

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)

EPO-Internal

**C. ALS WESENTLICH ANGESEHENE UNTERLAGEN**

Kategorie*	Bezeichnung der Veröffentlichung, soweit erforderlich unter Angabe der in Betracht kommenden Teile	Betr. Anspruch Nr.
A	DE 39 02 537 A (DAIMLER BENZ AG ; HUELSBECK & FUERST (DE)) 9. August 1990 (1990-08-09) in der Anmeldung erwähnt das ganze Dokument	1
A	EP 0 267 429 A (SIEMENS AG) 18. Mai 1988 (1988-05-18) in der Anmeldung erwähnt das ganze Dokument	1
A	US 4 726 205 A (ALLERDIST HEINZ ET AL) 23. Februar 1988 (1988-02-23) Spalte 1, Zeile 31 - Zeile 62 Spalte 2, Zeile 20 - Zeile 38; Abbildung	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

\*F\* 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 erfindersicher Tätigkeit beruhend betrachtet werden

\*Y\* Veröffentlichung von besonderer Bedeutung; die beanspruchte Erfindung kann nicht als auf erfindersicher 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

\*Z\* Veröffentlichung, die Mitglied derselben Patentfamilie ist

Datum des Abschlusses der internationalen Recherche

16. März 2001

Absenddatum des internationalen Recherchenberichts

26/03/2001

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

Pieracci, A

# INTERNATIONALER RECHERCHENBERICHT

Angaben zu Veröffentlichungen, die zur selben Patentfamilie gehören

Internationales Aktenzeichen

PCT/EP 00/12431

Im Recherchenbericht angeführtes Patentdokument	Datum der Veröffentlichung	Mitglied(eri) der Patentfamilie	Datum der Veröffentlichung
DE 3902537 A	09-08-1990	KEINE	
EP 0267429 A	18-05-1988	DE 3769923 D	13-06-1991
		JP 63110377 A	14-05-1988
		US 4888970 A	26-12-1989
US 4726205 A	23-02-1988	DE 3509579 A	18-09-1986
		DE 3678983 D	06-06-1991
		EP 0195195 A	24-09-1986
		JP 61229079 A	13-10-1986

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
23 August 2001 (23.08.2001)

PCT

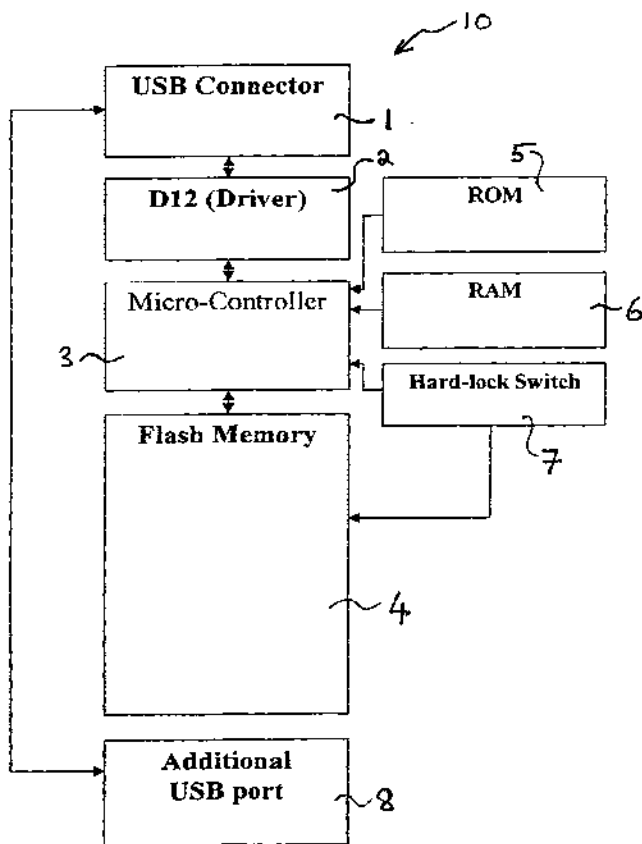
(10) International Publication Number  
WO 01/61692 A1

- (51) International Patent Classification: G11B 11/00
- (21) International Application Number: PCT/SG00/00029
- (22) International Filing Date: 21 February 2000 (21.02.2000)
- (25) Filing Language: English
- (26) Publication Language: English
- (71) Applicant (for all designated States except US): TREK TECHNOLOGY (SINGAPORE) PTE LTD [SG/SG]; 30 Loyang Way #07-13/14/15, Loyang Industrial Estate, Singapore 508769 (SG).
- (72) Inventor; and
- (75) Inventor/Applicant (for US only): CHENG, Chong, Seng [SG/SG]; 129 Loyang Rise, Singapore 507472 (SG).
- (74) Agent: MCCALLUM, Graeme, David; Lloyd Wise, Tanjong Pagar, P.O. Box 636, Singapore 910816 (SG).
- (81) Designated States (national): AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, 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, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW.
- (84) Designated States (regional): 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

[Continued on next page]

(54) Title: A PORTABLE DATA STORAGE DEVICE



(57) Abstract: A portable data storage device (10) includes a universal serial bus (USB) coupling device (1) and an interface device (2) is coupled to the USB coupling device (1). The portable data storage device (10) also includes a memory control device (3) and a non-volatile solid-state memory device (4). The memory control device (3) is coupled between the interface device (2) and the memory device (4) to control the flow of data from the memory device (4) to the USB coupling device (1).



WO 01/61692 A1





*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.*

## A Portable Data Storage Device

The invention relates to a portable data storage device, and in particular, a portable data storage device for a computer.

5

Conventional data storage devices generally fall into two categories. The first category is electronic, solid-state memory devices such as read only memory (ROM) and random access memory (RAM). These memory devices are generally fitted within the computer. They are not intended to be removable or portable so that they may be used on different computers, for example, to permit the transfer of data from one computer to another computer.

10

The second type of device is surface based data storage devices in which data is stored, typically, on the surface of a disk or tape. Examples of surface storage devices are magnetic disks and CD ROMs. Such data storage devices require a mechanical drive mechanism to be installed in or coupled to the computer to permit the data on the storage device to be read by the computer. In addition, such memory devices are limited by the surface area of the storage device, and the combination of the storage device and the drive mechanism for reading data from the storage device is generally bulky and/or delicate due to the moving parts that are required within the drive mechanism and/or storage device.

15  
20

In accordance with the present invention, there is provided a portable data storage device comprising a coupling device for coupling to a computer serial

25

bus, an interface device coupled to the coupling device, a memory control device and a non-volatile solid-state memory device; the memory control device being coupled between the interface device and the memory device to control the flow of data from the memory device to the coupling device.

5

An advantage of the invention is that by providing a portable data storage device comprising a coupling device with an interface device, memory control device and a non-volatile solid-state memory device, it is possible to provide a portable data storage device which may be coupled to a computer having a  
10 serial bus port and which does not include moving parts or require a mechanical drive mechanism to read the data from the data storage device.

Preferably, the non-volatile solid-state memory device may be a read/write memory device, such as a flash memory device.

15

Preferably, where the memory device is a read/write memory device, the memory control device controls the flow of data to and from the memory device.

Typically, the data storage device further comprises a manually operated switch  
20 movable between a first position in which writing of data to the memory device is enabled, and a second position in which writing of data to the memory device is prevented.

Preferably, the memory control device may include a read only memory which stores a program to control the operation of the memory control device.

Preferably, the memory control device is a micro-controller.

- 5 Typically, the interface device comprises a universal serial bus (USB) driver to convert data between a USB format and a PC format, and the coupling device comprises a USB coupling device.

- Alternatively, the interface device comprises a driver for IEEE 1394 (Firewire)  
10 protocol, and the coupling device comprises a Firewire coupling device.

An example of a data storage device in accordance with the invention will now be described to the accompanying drawings, in which:

- 15 Figure 1 is a schematic block diagram of a portable data storage device;  
Figure 2 is a flow diagram showing the initial setup of the data storage device by a software supplier;  
Figure 3 is a flow diagram showing the initial setup of the data storage device by an end user; and  
20 Figure 4 is a flow diagram showing operation of the data storage device.

Figure 1 shows a data storage device 10 which includes a USB plug 1 which is coupled to a USB interface device 2. The USB interface device 2 is coupled to a micro-controller 3 which is coupled to a flash memory 4. The micro-controller

3 includes a read only memory (ROM) 5 which stores a program to control the operation of the micro-controller 3.

The operations performed by the micro-controller 3 include comparing  
5 passwords entered by a user with a corresponding password stored in the flash memory 4 to determine whether the user is authorised to access the contents of the flash memory 4. The program stored in the ROM 5 also controls the data flow to and from the flash memory 4 and can also detect whether the computer to which the memory device 1 is coupled has installed software programs which  
10 correspond to passwords stored in the flash memory 4. The micro-controller 3 can automatically retrieve passwords from the installed software to compare with passwords stored in the flash memory to verify that a user of the computer is authorised to access and run the software. In addition, the program stored in the ROM 5 also permits the setting of a password in the flash memory by a  
15 software supplier to correspond to the password contained in software supplied to a user. Typically, the password may correspond to the serial number of the software.

The flash memory 4 is typically divided into a number of different sections or  
20 zones. Typically, the flash memory is divided into two zones and each zone has a unique password. If the data storage device 10 is supplied with packaged software, the software serial number can be set in one zone to be the password to permit a user to access and use the software. The other zone, which can be used typically for storing a user's data, may have a separate password which is  
25 set by the user. Typically, the passwords are stored in a secure location of the

flash memory in an encrypted form. The encryption, decryption, data flow control and USB protocol are all managed by the micro-controller 3.

The micro-controller 3 also includes a random access memory (RAM) 6 which is  
5 a temporary storage area to permit functioning of the micro-controller 3. In addition, a manual switch 7 is coupled between the flash memory 4 and the micro-controller 3. The manual switch 7 is movable between a first position in which a user may write data to the flash memory 4 and a second position in which data is prevented from being written to the flash memory 4.

10

The device 10 also includes a USB socket 8 that is coupled directly to the USB plug 1 and permits other USB devices to be coupled to the USB via the device 10. For example, if a user wishes to increase memory space, a USB plug 1 of a second memory device 10 may be connected to the USB socket 8.

15

Figure 2 is a flow diagram showing the set up procedure for the device 10 for a software supplier when the software supplier intends to supply the device as an authentication device for the software. Firstly, the plug 1 of the device 10 is plugged into 20 to a USB socket on a computer. After the device 10 has been plugged into the USB socket on the computer, a communication is established 21 between the computer and the device 10. The software supplier has pre-installed installation software on the computer which is run by the operator. From the pre-installed software, the operator selects password set up installation 22, in response to which the pre-installed software requests the  
25 operator to enter a password or serial number corresponding to the software

with which the device 10 is to be supplied. The password or serial number is then encrypted 26 and stored 27 in the flash memory 4.

Figure 3 is a flow diagram showing the initial set-up of a password for zone 2 of the flash memory 4 by an end user. The device 10 is typically supplied with driver software that is loaded by the user onto the computer prior to set-up of the device. To set-up the password for zone 2 the user plugs in 20 the device 10 into a USB port on the computer and communication 21 is established between the computer and the device 10. The user then runs the driver software and the driver software enters a password installation set-up mode 23 for zone 2. The user then enters 28 a password that they wish to use to prevent unauthorised access to zone 2 of the flash memory 4. The password entered is then encrypted 29 and stored 30 in the flash memory 4.

After an end user has performed the initial password set up procedure described above and shown in Figure 3, when a user plugs in 20 the device 10 to a USB port on a computer, the computer will establish a communication 21 with the device 10 and firstly, checks 33 an installation status flag stored in the flash memory 4 (see Figure 4). If the status flag is "Y", the device 10 outputs 34 an "OK" flag to the computer. The micro-controller 3 then instructs the computer to issue a request 35 to the user to select the zone they wish to enter. If the status flag is "N", the device does not output an "OK" flag to the computer, and goes straight to step 35. In response to the request 35 for zone selection, the user selects 36 either zone 1 or zone 2.

If zone 1 is selected, the device 10 assumes that the user wishes to install software on the computer which is stored in the flash memory 4 and requests 37 the appropriate password for confirmation that the user is authorised to install the software. The micro-controller 3 receives the password entered by the user, retrieves the zone 1 password stored in the flash memory 4, decrypts the zone 1 password and compares it with the password entered by the user to authenticate 38 whether the user is authorised to install the software. If the passwords do not match, the device 10 prompts the computer to request 37 the user to enter the password again.

10

If the password entered by the user matches the password stored in the flash memory 4, the micro-controller 3 starts 39 the software installation from the flash memory 4 to the computer. In order to install software, the computer sends 40 a read/write command in USB format to the micro-controller 3 for data, the micro-controller 3 retrieves the requested data from the flash memory 4 and sends 41 the data to the driver 2. The driver 2 converts 42 the data to PC format and outputs the data to the computer through the USB plug 1. The micro-controller 3 then checks 43 whether the software installation is complete. If the operation is not complete, the operation returns to step 40. If the installation of the software is complete, the status flag stored in the flash memory 4 is changed to "Y" and the device 10 may then be removed 45 from the USB socket on the computer.

If a user selects zone 2, the micro-controller 3 sends a command to the computer to request 46 the user to enter the password for zone 2. When the

25



user enters the password, the computer sends the password to the micro-controller 3. The micro-controller 3 retrieves the password for zone 2 from the flash memory 4, decrypts 47 the password and compares it with the password entered by the user. If the password entered by the user is incorrect, the  
5 operation returns to step 46 and the computer requests 46 the user for the password again.

If the password entered by the user is correct, the user has access to zone 2 of the flash memory 4 to read data from the flash memory 4 and to write data to  
10 the flash memory 4. However, data can only be written to the flash memory 4 if the manual switch 7 is in the position to permit data to be written to the flash memory 4. In order to read or write data from or to the flash memory 4 a read or write command is sent 48 by the computer in USB format to the micro-controller 3. In response to the read or write command the micro-controller 3  
15 either retrieves 49 data from the flash memory 4 and sends it to the driver 2 for conversion 50 to PC format and then to be output to the computer or receives data from the driver to write it to the flash memory 4.

The micro-controller 3 then determines 51 whether the read or write operation is  
20 complete. If the operation is not complete it returns to step 48. If the operation is complete the operation terminates 52.

The device 10 described above is for coupling to a universal serial bus (USB). However, the plug 1, the interface device 2 and socket 8 could be for use with  
25 any appropriate computer serial bus. For example, the device 10 could be

modified for use with IEEE 1394 (Firewire) protocol by substituting the USB plug 1, USB interface device 2 and socket 8 with a Firewire protocol compatible plug, interface device and socket respectively.

- 5 An advantage of the device 10 described above is that it provides a portable data storage device for a computer which does not require a mechanical operated reading/writing device. In addition, the device 10 has no moving parts. This enables to data storage device 10 to be more compact than conventional portable data storage devices.

**CLAIMS**

1. A portable data storage device comprising a coupling device for coupling to a computer serial bus, an interface device coupled to the coupling device, a memory control device and a non-volatile solid-state memory device; the  
5 memory control device being coupled between the interface device and the memory device to control the flow of data from the memory device to the coupling device.
2. A device according to claim 1, wherein the non-volatile solid-state  
10 memory device is a read/write memory device.
3. A device according to claim 2, wherein the read/write memory device is a flash memory device.
- 15 4. A device according to claim 2 or claim 3, wherein the memory control device controls the flow of data to and from the memory device.
5. A device according to any of claims 2 to 4, further comprising a manually operated switch movable between a first position in which writing of data to the  
20 memory device is enabled, and a second position in which writing of data to the memory device is prevented.
6. A device according to any of the preceding claims, wherein the memory control device comprises a micro-controller.

7. A device according to any of the preceding claims, wherein the coupling device comprises a universal serial bus coupling device and the interface device comprises a USB driver.
  
- 5 8. A device according to any of the preceding claims, wherein the coupling device comprises an IEEE 1394 (Firewire) protocol coupling device and the interface device is a Firewire protocol driver.

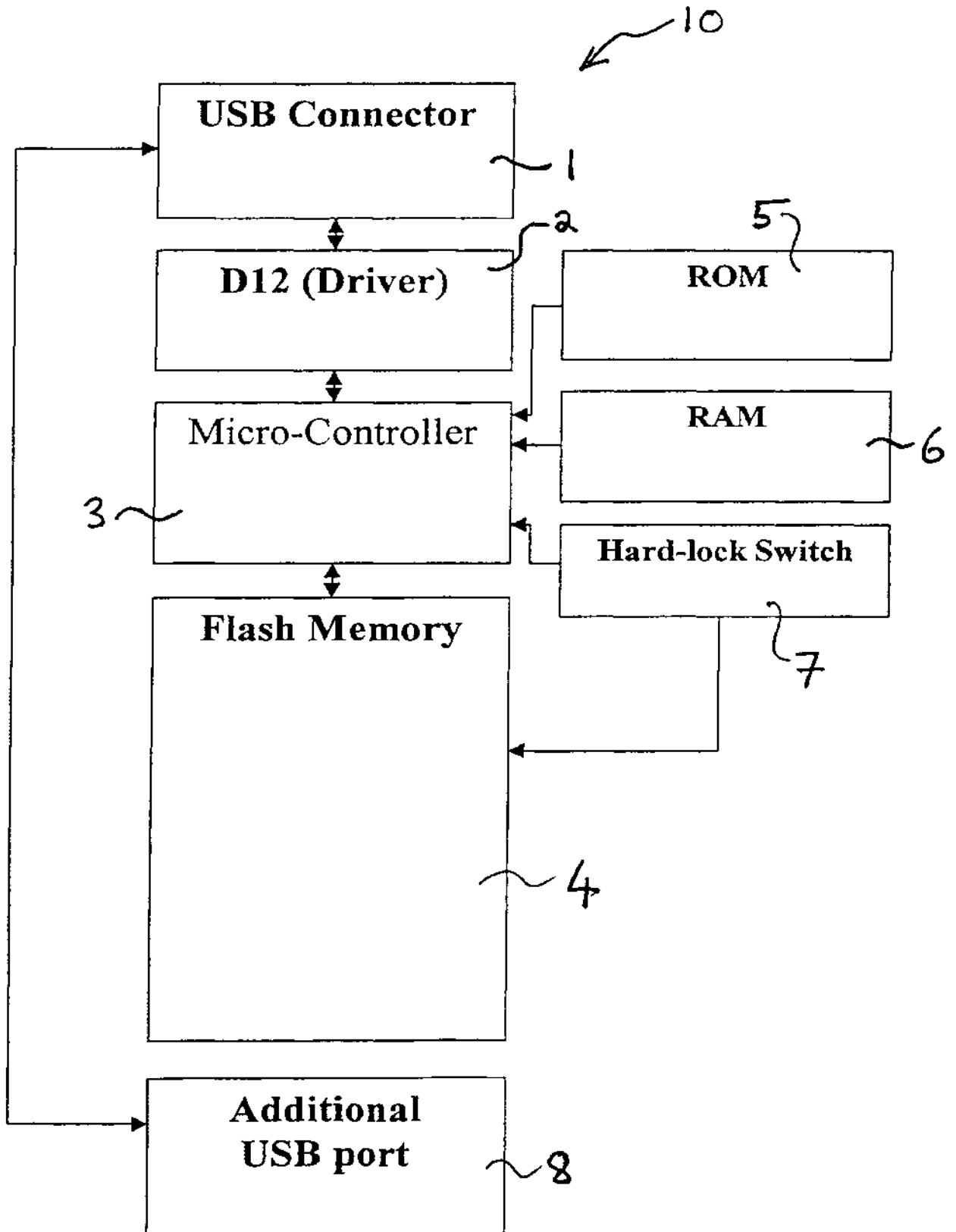


Figure 1

2 / 3

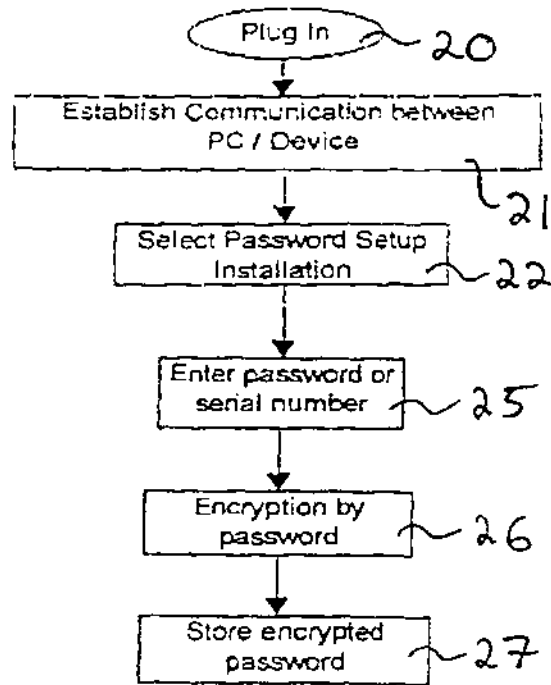


Figure 2

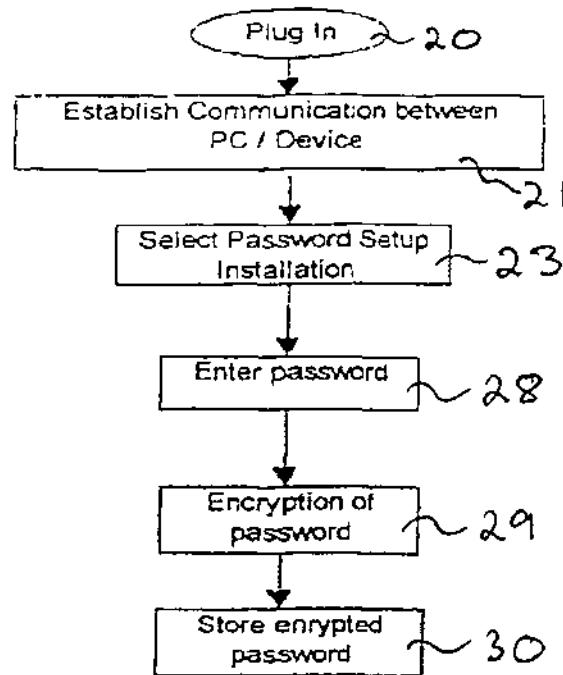


Figure 3

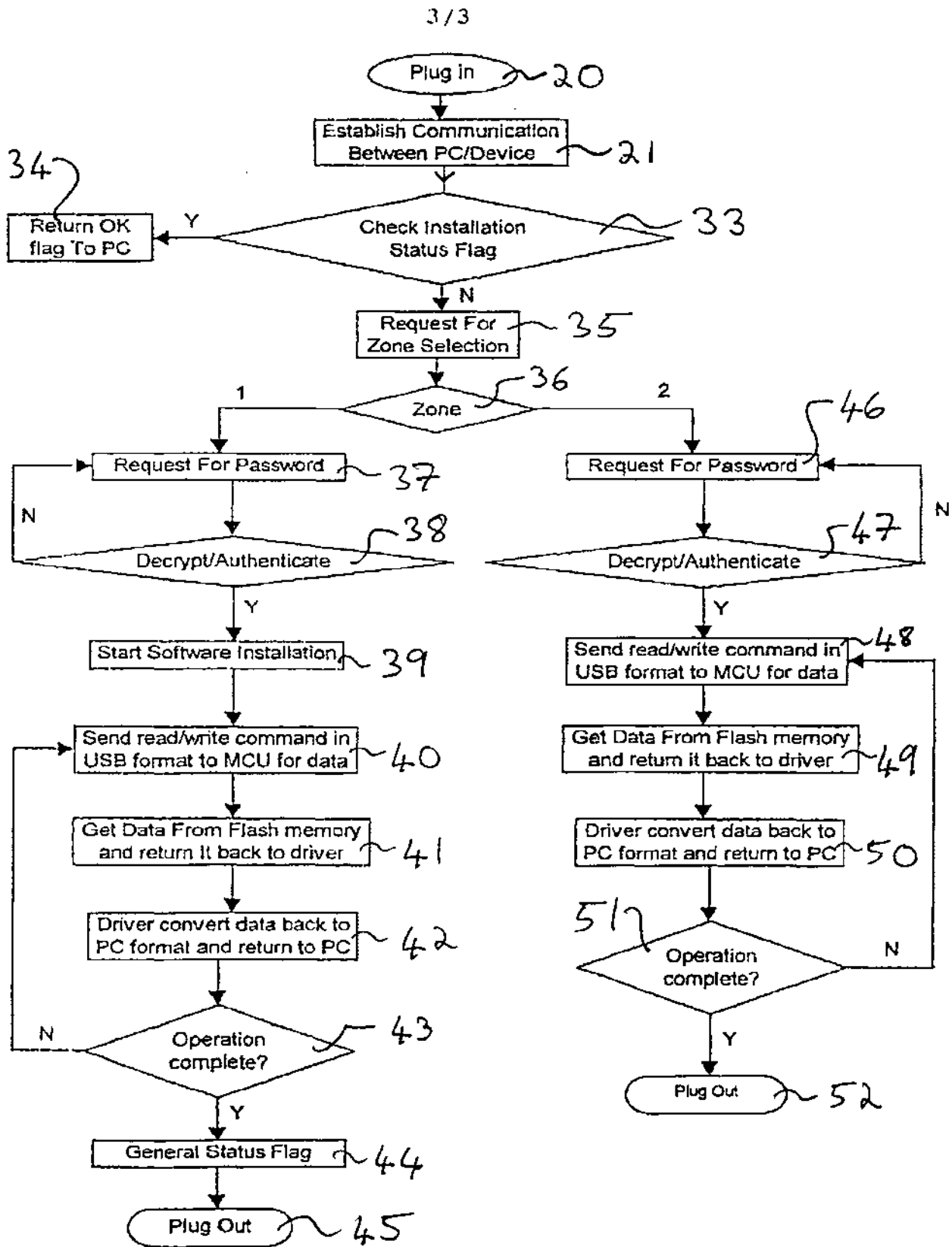


Figure 4

**INTERNATIONAL SEARCH REPORT**

International application No.  
PCT/SG 00/00029

**CLASSIFICATION OF SUBJECT MATTER**

IPC<sup>7</sup>: G11B 11/00

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<sup>7</sup>: G11B 11/00, 02,05

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

G06F 3/00, 12/00, 12/06

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

WPI

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 6016530 A (AUCLAIR et al.) 18 January 2000 (18.01.00)	1
P,A	US 6058441 A (SHU) 2 May 2000 (02.05.00)	1
A	US 5760986 A (MOREHOUSE et al.) 2 June 1998 (02.06.98)	1
	---	

Further documents are listed in the continuation of Box C.

See patent family annex.

\* Special categories of cited documents:

„A“ document defining the general state of the art which is not considered to be of particular relevance

„E“ earlier application or patent 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

24 March 2001 (24.03.2001)

Date of mailing of the international search report

12 April 2001 (12.04.2001)

Name and mailing address of the ISA/AT

Austrian Patent Office  
Kohlmarkt 8-10; A-1014 Vienna  
Facsimile No. 1/53424/535

Authorized officer

GROSSING

Telephone No. 1/53424/386



**INTERNATIONAL SEARCH REPORT**  
Information on patent family members

International application No.  
PCT/SG 00/00029

Patent document cited in search report			Publication date	Patent family member(s)			Publication date
US	A	5760986	01-06-1998	EP	A1	614564	14-09-1994
				EP	A4	614564	19-07-1995
				US	A	5379171	03-01-1995
				WO	A1	9306594	01-04-1993
				US	A	5835303	10-11-1998
				US	A	5579189	26-11-1996
				US	A	5592349	07-01-1997
				US	A	5694267	02-12-1997
				US	A	5867340	02-02-1999
				US	A	6016530	18-01-2000
US	A	6058441	02-05-2000	none			

(12) NACH DEM VERTRAG ÜBER DIE INTERNATIONALE ZUSAMMENARBEIT AUF DEM GEBIET DES PATENTWESENS (PCT) VERÖFFENTLICHTE INTERNATIONALE ANMELDUNG

(19) Weltorganisation für geistiges Eigentum  
Internationales Büro



(43) Internationales Veröffentlichungsdatum  
22. November 2001 (22.11.2001)

PCT

(10) Internationale Veröffentlichungsnummer  
**WO 01/88693 A2**

(51) Internationale Patentklassifikation<sup>7</sup>: **G06F 7/72**  
(21) Internationales Aktenzeichen: PCT/EP01/05532  
(22) Internationales Anmeldedatum:  
15. Mai 2001 (15.05.2001)  
(25) Einreichungssprache: Deutsch  
(26) Veröffentlichungssprache: Deutsch  
(30) Angaben zur Priorität:  
100 24 325.8 17. Mai 2000 (17.05.2000) DE  
(71) Anmelder (für alle Bestimmungsstaaten mit Ausnahme von US): **GIESECKE & DEVRIENT GMBH** [DE/DE]; Prinzregentenstrasse 159, 81677 München (DE).

(81) Bestimmungsstaaten (national): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, 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, US, UZ, VN, YU, ZA, ZW.

(84) Bestimmungsstaaten (regional): ARIPO-Patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZW), eurasisches Patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), europäisches 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).

**Veröffentlicht:**

*ohne internationalen Recherchenbericht und erneut zu veröffentlichen nach Erhalt des Berichts*

*Zur Erklärung der Zweibuchstaben-Codes und der anderen Abkürzungen wird auf die Erklärungen ("Guidance Notes on Codes and Abbreviations") am Anfang jeder regulären Ausgabe der PCT-Gazette verwiesen.*

(72) Erfinder; und  
(75) Erfinder/Anmelder (nur für US): **SEYSEN, Martin** [DE/DE]; Scheissheimer Strasse 339, 80809 München (DE).  
(74) Anwalt: **KLUNKER, SCHMITT-NILSON, HIRSCH**; Winzererstrasse 106, 80797 München (DE).



**WO 01/88693 A2**

(54) Title: CRYPTOGRAPHIC METHOD AND CRYPTOGRAPHIC DEVICE

(54) Bezeichnung: KRYPTOGRAPHISCHES VERFAHREN UND KRYPTOGRAPHISCHE VORRICHTUNG

(57) Abstract: The invention relates to a cryptographic method comprising at least one arithmetic step which contains a modular exponentiation E, according to the equation  $E=x^d \pmod{p \cdot q}$ , comprising a first prime factor p, a second prime factor q, an exponent d and a number x. According to said method, the modular exponentiation E is calculated according to the Chinese Remainder Theorem.

(57) Zusammenfassung: Die Erfindung betrifft ein kryptographisches Verfahren mit mindestens einem eine modulare Exponentiation E gemäss  $E=x^d \pmod{p \cdot q}$  enthaltenden Rechenschritt mit einem ersten Primfaktor p, einem zweiten Primfaktor q, einem Exponenten d und einer Zahl x, wobei die modulare Exponentiation E gemäss dem Chinesischen Restwertsatz berechnet wird.

Kryptographisches Verfahren und kryptographische Vorrichtung

Kryptographische Verfahren in Gestalt von Verschlüsselungs- und Signaturverfahren erfreuen sich insbesondere durch die steigende Bedeutung des elektronischen Geschäftsverkehrs einer stetig wachsenden Verbreitung. Sie werden in der Regel mittels elektronischer Vorrichtungen implementiert, die beispielsweise einen programmierbaren universellen Mikrokontroller oder auch eine spezialisierte elektronische Schaltung etwa in Gestalt eines ASIC beinhalten können. Eine besonders interessante Form kryptographischer Vorrichtungen ist die Chipkarte, da sich in ihr bei zweckdienlicher technischer Ausgestaltung geheime Schlüsseldaten gegen unbefugten Zugriff schützen lassen. Ein ständiges Bemühen gilt dabei sowohl der Verbesserung der Ausführungsgeschwindigkeit der kryptographischen Verfahren als auch deren Sicherung gegen alle denkbaren Arten von Angriffen. Die Erfindung eignet sich insbesondere für den Einsatz im Zusammenhang mit Chipkarten, ist aber in keiner Weise darauf beschränkt. Sie ist vielmehr im Zusammenhang mit allen Arten von kryptographischen Vorrichtungen implementierbar.

Bei einer Reihe bekannter kryptographischer Verfahren ist es erforderlich, eine modulare Exponentiation gemäß der Gleichung

$$E = x^d \pmod{N} = x^d \pmod{p \cdot q} \quad (1)$$

durchzuführen, wobei  $p$  und  $q$  Primzahlen sind. Ein besonders bedeutendes kryptographisches Verfahren, welches einen modularen Exponentiationsschritt beinhaltet, ist das beispielsweise aus Alfred J. Menezes, Paul C. van Oorschot und Scott A. Vanstone, "Handbook of Applied Cryptography", Boca Raton: CRC Press, 1997, Seiten 285 bis 291, bekannte RSA-Verfahren. Die Verwendung der modularen Exponentiation ist jedoch nicht auf das RSA-Verfahren beschränkt, sondern umfaßt beispielsweise auch aus Menezes et al., a.a.O., Seiten 438 bis 442, bekannte Rabin-Signaturen und das aus Mene-

zes et al., a.a.O., Seite 408 bis 410, bekannte Fiat-Shamir'sche Identifikations-schema.

Die Sicherheit von kryptographischen Verfahren, die die modulare Exponentiation einbeziehen, ist regelmäßig abhängig von der Schwierigkeit, die Zahl  
 5 N aus Gleichung (1) in ihre Primfaktoren p und q zerlegen zu können. Dieses Problem ist nur für hinreichend große Werte N von ausreichender Komplexität, so daß einerseits N möglichst groß gewählt werden sollte. Der Rechenaufwand zur Berechnung von Werten mittels modularer Exponentiation  
 10 gemäß Gleichung (1) steigt andererseits monoton mit der Größenordnung von N, so daß es unter dem Gesichtspunkt der praktischen Anwendbarkeit wünschenswert wäre, trotz großer Werte von N den Rechenzeitaufwand auf akzeptable Werte beschränken zu können.

15 Es ist bekannt, durch Anwendung des sog. "Chinesischen Restwertsatzes" die Rechengeschwindigkeit um einen Faktor 4 erhöhen zu können, wodurch beispielsweise bei gleicher Rechenzeit größere Werte N zugelassen werden können. Statt unmittelbar die Gleichung (1) auszuwerten, wird eine Umformung vorgenommen gemäß

$$20 \quad E = x^d \pmod{p \cdot q} = aE_1 + bE_2 \pmod{N} \quad (2)$$

mit

$$E_1 = x^d \pmod{p} \quad (3)$$

$$E_2 = x^d \pmod{q} \quad (4)$$

25 Eine Folge der Anwendung des Chinesischen Restwertsatzes besteht darin, daß die modulare Exponentiation nicht mehr modulo N, also modulo derjenigen Zahl, die ihre eigene Primfaktorzerlegung noch in sich verbirgt, sondern nacheinander in einem ersten Teilschritt modulo p und in einem zweiten Teilschritt modulo q erfolgt, d.h. die Kenntnis der geheimzuhaltenden

- Primfaktorzerlegung  $n = p \cdot q$  wird bei dieser Rechenvorschrift vorausgesetzt und führt zu einer Aufteilung des Gesamtrechenprozesses in einen ersten Rechenschritt (3), in den der erste Primfaktor wesentlich eingeht, und einen zweiten Rechenschritt (4), in den der zweite Primfaktor wesentlich eingeht.
- 5 Der Vorteil hierbei liegt darin, daß der Exponent  $d$  in Gleichung (1) modulo  $\phi(p \cdot q)$  definiert sein muß, wohingegen die Exponenten in Gleichung (2) lediglich modulo  $\phi(p)$  bzw.  $\phi(q)$  definiert sein müssen, wobei mit  $\phi$  die Euler'sche Funktion notiert ist.
- 10 Interessanterweise ist nun in der letzten Zeit ein Angriffsschema auf solche kryptographischen Verfahren, die die modulare Exponentiation nutzen, bekannt geworden, bei dem durch einen geeigneten artifiziellen Eingriff in den ansonsten störungsfreien Rechenablauf aus dem fehlerhaften Ergebnis einer gestörten modularen Exponentiation die Information über die Primfaktor-
- 15 zerlegung von  $N$  zurückgewonnen werden kann, sofern die konkrete Implementation von dem Chinesischen Restwertsatz gemäß den Gleichungen (2) bis (4) Gebrauch macht. Dieser als "Bellcore-Angriff" bekannte Versuch ist beispielsweise in Dan Boneh, Richard A. DeMillo und Richard J. Lipton: "On the importance of checking Cryptographic Protocols for Faults", Advances in
- 20 Cryptology -EUROCRYPT, 97, Lecture Notes in Computer Science 1233, Berlin: Springer, 1997 beschrieben. Eine Verschlüsselungseinrichtung wird durch physikalische Eingriffe wie beispielsweise Übertaktung, zu hohe Betriebsspannung oder Bestrahlung manipuliert, so daß mit einer gewissen, nicht zu großen Wahrscheinlichkeit Rechenfehler bei der Ausführung der
- 25 modularen Exponentiation nach dem Chinesischen Restwertsatz auftreten. Wenn ein Rechenfehler nur bei einem der beiden Terme in Gleichung (2) auftritt, können die beiden Primfaktoren  $p$  und  $q$  aus dem fehlerbehafteten Exponentiationsergebnis rekonstruiert werden.

Die aus dieser Verletzlichkeit der mittels des Chinesischen Restwertsatzes implementierten modularen Exponentiation zu ziehende Konsequenz besteht darin, das Ergebnis des Rechenvorganges zuerst auf seine Korrektheit zu prüfen, bevor es weiterverarbeitet, insbesondere aber bevor es in irgend  
 5 einer Form, etwa in Gestalt einer Signatur, ausgegeben wird.

Ein triviales Gegenmittel gegen den "Bellcore-Angriff" besteht darin, diese Korrektheitsprüfung dadurch zu bewerkstelligen, indem der Rechenvorgang mindestens einmal wiederholt wird. Bei zufälligen Rechenfehlern kann da-  
 10 von ausgegangen werden, daß das Ergebnis des ersten Rechenganges von demjenigen der Kontrollrechengänge abweicht. Der wesentliche Nachteil dieses Ansatzes besteht darin, daß sich die Rechenzeit bereits bei einer Kontrollrechnung verdoppelt.

15 Aus der Druckschrift WO-A1-98/52319 ist insbesondere ein Verfahren zum Schutz von eine modulare Exponentiation nach dem Chinesischen Restwertsatz ausführenden Rechenoperationen gegen den "Bellcore-Angriff" bekannt. Dabei wird eine geheime ganz Zahl  $j$  beispielsweise im Bereich  $[0, 2^k-1]$  mit  $16 \leq k \leq 32$  ausgewählt. Sodann werden folgende Ausdrücke berechnet:

$$20 \quad v_1 = x \pmod{j \cdot q} \quad (5)$$

$$v_2 = x \pmod{j \cdot q} \quad (6)$$

$$d_1 = d \pmod{\phi(j \cdot p)} \quad (7)$$

$$d_2 = d \pmod{\phi(j \cdot q)} \quad (8)$$

$$w_1 = v_1^{d_1} \pmod{j \cdot p} \quad (9)$$

$$25 \quad w_2 = v_2^{d_2} \pmod{j \cdot q} \quad (10)$$

Sodann wird geprüft, ob gilt:

$$w_1 = w_2 \pmod{j} \quad (11)$$

Kann der Ausdrücke (11) verifiziert werden, so werden bei dem bekannten Verfahren folgende Ausdrücke berechnet:

$$5 \quad y_1 = w_1 \pmod{p} \quad (12)$$

$$y_2 = w_2 \pmod{q} \quad (13)$$

woraus dann mittels des Chinesischen Restwertsatzes der Wert für

$$E = x^d \pmod{N} \quad (14)$$

ermittelt werden kann.

10

Dieses bekannte Verfahren weist gegenüber einfachen Kontrollrechengängen den Vorteil auf, daß der zusätzliche Rechenzeitaufwand wesentlich geringer ist.

15

Bei diesem Verfahren müssen beide Primzahlen  $p$  und  $q$  mit demselben Faktor  $d$  multipliziert werden. In der Druckschrift WO-A1-98/52319 ist ein zweites Verfahren beschrieben, welches es erlaubt, die Primzahlen  $p$  und  $q$  mit verschiedenen Faktoren  $r$  und  $s$  zu multiplizieren. Hierbei sind jedoch für die Kontrollrechnung zwei weitere Exponentiationen möglich.

20

Aufgabe der Erfindung ist es, ein kryptographisches Verfahren bzw. eine kryptographische Vorrichtung anzugeben, bei dem bzw. bei der unter Beibehaltung oder Erhöhung der Sicherheit Rechenoperationen oder Rechenzeit eingespart werden kann.

25

Diese Aufgabe wird erfindungsgemäß gelöst durch ein kryptographisches Verfahren mit den in Anspruch 1 oder 2 angegebenen Merkmalen als auch durch eine kryptographische Vorrichtung mit den in Anspruch 13 oder 14 angegebenen Merkmalen.

Den abhängigen Ansprüchen 3 bis 12 sowie 15 bis 24 sind vorteilhafte Weiterbildungen entnehmbar.

- 5 Wie weiter unten erwähnt wird, ist es auf bestimmten Rechenwerken vorteilhaft, wenn ein Modulus bei der modularen Exponentiation viele führende binäre Einsen besitzt, so daß verschiedene Faktoren  $r$  und  $s$  hier einen gewissen Vorteil bedeuten. Ferner gibt es für die modulare Exponentiation optimierte Rechenwerke, wobei aber allein der Datentransfer von der Zentral-
- 10 traleinheit in das optimierte Rechenwerk für die Exponentiation einen beträchtlichen Verwaltungsaufwand verursacht. Die vorliegende Erfindung spart gegenüber dem oben beschriebenen Verfahren bei verschiedenen Faktoren  $r$  und  $s$  eine Exponentiation ein.

- 15 Erfindungsgemäß werden zwei ganze Zahlen  $r$  und  $s$  beispielsweise im Bereich  $[0, 2^k-1]$  mit  $16 \leq k \leq 32$  ausgewählt, so daß  $d$  teilerfremd zu  $\phi(\text{kgV}(r,s))$  ist, wobei  $\text{kgV}(r,s)$  das kleinste gemeinsame Vielfache von  $r$  und  $s$  angibt, und  $\phi()$  die Euler'sche Funktion darstellt. Sodann werden folgende Ausdrücke berechnet:

20 
$$x_1 = x \pmod{p \cdot r} \quad (15)$$

$$x_2 = x \pmod{q \cdot s} \quad (16)$$

$$d_1 = d \pmod{\phi(p \cdot r)} \quad (15)$$

$$d_2 = d \pmod{\phi(q \cdot s)} \quad (16)$$

$$z_1 = x_1^{d_1} \pmod{p \cdot r} \quad (15)$$

25 
$$z_2 = x_2^{d_2} \pmod{q \cdot s} \quad (16)$$

Jetzt gilt  $z_1 = x^d \pmod{p \cdot r}$  und  $z_2 = x^d \pmod{q \cdot s}$ . Nach dem Chinesischen Restwertsatz läßt sich aus  $z_1$  und  $z_2$  leicht eine Zahl  $z$  berechnen mit



$$z = z_1 \pmod{p \cdot r} ; z = z_2 \pmod{q \cdot s} ; z = x^d \pmod{p \cdot q \cdot \text{kgV}(r,s)} \quad (17)$$

Die Zahlen  $r$  und  $s$  müssen erfindungsgemäß so gewählt werden, daß  $d$  teilerfremd ist zu  $\phi(\text{kgV}(r,s))$ . Unter diesen Umständen läßt sich mit Hilfe des erweiterten Euklid'schen Algorithmus leicht eine natürliche Zahl  $e$  finden mit

$$e \cdot d = 1 \pmod{\phi(\text{kgV}(r,s))} \quad (18)$$

Mit Hilfe von  $Z$  und  $e$  wird die Zahl  $C$  wie folgt berechnet:

$$C = z^e \pmod{\text{kgV}(r,s)} \quad (19)$$

Nach dem Satz von Euler gilt:

$$10 \quad C = x^{d \cdot e} = x \pmod{\text{kgV}(r,s)} \quad (20)$$

Durch Vergleich der beiden Werte  $C$  und  $x$  modulo  $\text{kgV}(r,s)$  läßt sich ein Fehler mit hoher Wahrscheinlichkeit feststellen. Wenn  $C \neq x \pmod{\text{kgV}(r,s)}$  festgestellt wird, ist das Ergebnis der modularen Exponentiation als fehlerbehaftet anzusehen und zu verwerfen.

15

Bei RSA-Verfahren (ebenso wie beim Rabin'schen Signaturverfahren) ist zur Erzeugung einer digitalen Signatur oder zur Entschlüsselung eine modulare Exponentiation durchzuführen, wobei der Modulus  $p \cdot q$  und Exponent  $d$  nur vom privaten Schlüssel abhängen. Infolgedessen können die Zahlen  $d$ ,  $e$ ,  $r$  und  $s$  einmal beim Einbringen des privaten Schlüssel berechnet und zur Wiederverwendung abgespeichert werden.

20

In einer Variante der Erfindung werden ebenfalls zwei ganze Zahlen  $r$  und  $s$  beispielsweise im Bereich  $[0, 2^k - 1]$  mit  $16 \leq k \leq 32$  ausgewählt. Auf einem binären Rechenwerk wird empfohlen, daß die Zahlen  $r$  und  $s$  beide ungerade sind. Außerdem werden zwei feste, nicht von  $x$  abhängige Zahlen  $b_1$  und  $b_2$  im Intervall  $[1, \dots, r-1]$  bzw.  $[1, \dots, s-1]$  und teilerfremd zu  $r$  bzw.  $s$  gewählt. Falls  $r$  und  $s$  nicht teilerfremd sind, müssen  $b_1$  und  $b_2$  die zusätzliche Bedin-

25

gung  $b_1 = b_2 \pmod{\text{ggT}(r,s)}$  erfüllen, wobei  $\text{ggT}(r,s)$  den größten gemeinsamen Teiler von  $r$  und  $s$  bezeichnet.

Nach dem Chinesischen Restsatz wird zunächst eine Zahl  $x_1$  berechnet mit

$$5 \quad x_1 = x \pmod{p} , \quad x_1 = b_1 \pmod{r} \quad (21)$$

Ebenso wird eine Zahl  $x_2$  berechnet mit

$$x_2 = x \pmod{q} , \quad x_2 = b_2 \pmod{s} \quad (22)$$

Sodann werden folgende Ausdrücke berechnet:

$$10 \quad d_1 = d \pmod{\phi(p)} \quad (23)$$

$$d_2 = d \pmod{\phi(q)} \quad (24)$$

$$z_1 = x_1^{d_1} \pmod{p \cdot r} \quad (25)$$

$$z_2 = x_2^{d_2} \pmod{q \cdot s} \quad (26)$$

$$C_1 = b_1^{d_1} \pmod{r} \quad (27)$$

$$15 \quad C_2 = b_2^{d_2} \pmod{s} \quad (28)$$

Zur Einsparung von Rechenzeit können die Exponenten  $d_1$  und  $d_2$  in (27) bzw. (28) vor der Durchführung der Exponentiation modulo  $\phi(r)$  bzw.  $\phi(s)$  reduziert werden.

20 Aus (23) und (25) folgt

$$z_1 = x^d \pmod{p} \quad (29)$$

Aus (24) und (26) folgt

$$z_2 = x^d \pmod{q}. \quad (30)$$

25 Nach dem Chinesischen Restwertsatz läßt sich aus  $z_1$  und  $z_2$  leicht eine Zahl  $z$  berechnen mit

$$z = z_1 \pmod{p \cdot r} ; \quad z = z_2 \pmod{q \cdot s} ; \quad (31)$$

Selbst wenn  $r$  und  $s$  nicht teilerfremd sind, existiert eine solche Zahl  $z$  wegen  $z_1 = C_1 = b_1^{d \cdot 1} = b_2^{d \cdot 2} = C_2 = z_2 \pmod{\text{ggT}(r,s)}$ . Da  $p$  und  $q$  teilerfremd sind, folgt aus (29), (30) und (31):

$$z = x^d \pmod{p \cdot q}. \quad (32)$$

- 5 so daß sich die gesuchte Zahl  $z$  leicht aus den oben berechneten Werten ermitteln läßt.

Aus (21), (25) und (27) folgt

$$z_1 = C_1 \pmod{r} \quad (33)$$

- 10 Aus (22), (26) und (28) folgt

$$z_2 = C_2 \pmod{s}. \quad (34)$$

- Durch Prüfung der Bedingungen (33) und (34) läßt sich ein Fehler mit hoher Wahrscheinlichkeit feststellen. Wenn eine der Bedingungen (33) oder (34)  
 15 verletzt wird, ist das Ergebnis der modularen Exponentiation als fehlerbehaftet anzusehen und zu verwerfen.

- Im Gegensatz zu dem Verfahren in Patentanspruch 8 der Druckschrift WO-A1-98/52319 sind die Zahlen  $b_1$  und  $b_2$  in der hier vorgestellten Variante des  
 20 Verfahrens nicht von der Basis  $x$  abhängig. Typischerweise wird bei der Anwendung des RSA-Verfahrens oder des Rabin'schen Signaturverfahrens ein privater Schlüssel einmal in ein kryptographisches Gerät, z. B. in eine Chipkarte eingebracht, und anschließend mehrmals verwendet. Hierbei ist  
 25 bei der in diesen Verfahren angewendeten modularen Exponentiation der Exponent  $d$  sowie der Modulus  $p \cdot q$  jeweils ein fester Bestandteil des privaten Schlüssels. Infolgedessen müssen die Werte  $C_1$  und  $C_2$  nur einmal beim Einbringen des Schlüssels in das kryptographische Gerät berechnet werden, und können dann anschließend in dem Gerät abgespeichert werden. Das

Abspeichern dieser Werte spart ggü. dem in der Druckschrift WO-A1-98/52319 vorgestellten Verfahren zwei modulare Exponentiationen.

Eine kryptographische Vorrichtung, beispielsweise eine Chipkarte, mit einer  
5 Zusatzhardware für die Beschleunigung der modularen Arithmetik enthält  
bei üblichen Ausführungsformen schnelle Addier- und/oder Multipli-  
ziereinheiten, während die bei der modularen Reduktion erforderliche Divi-  
sion durch eine lange Zahl nach üblichen Standardverfahren durchgeführt  
werden muß, wie sie beispielsweise aus Donald Knuth: "The Art of Compu-  
10 ter Programming", Volume 2: Seminumerical Algorithms, 2. Ed., Addison-  
Wesley, 1981, bekannt sind. Eines von mehreren bekannten Verfahren zur  
Vereinfachung der Divisionsoperation besteht darin, den Modulus  $p$  vor der  
Exponentiation mit einer Zahl  $r$  zu multiplizieren, so daß die Binärdarstel-  
lung des Produktes  $p \cdot r$  möglichst viele Einsen enthält; siehe beispielsweise  
15 Menezes et al. a.a.O., Seiten 598 bis 599. Die Division durch eine Zahl mit  
möglichst vielen führenden Einsen ist erheblich einfacher als die Division  
durch eine allgemeine Zahl.

Der Multiplikator  $r$  wird erfindungsgemäß so gewählt, daß  $d$  teilerfremd zu  
20  $\phi(r)$  ist. Bei der o.g. Variante der Erfindung ist diese Teilerfremdheit nicht  
erforderlich. Für jeden Modulus  $p$  gibt es einen von der jeweiligen techni-  
schen Implementierung der Division abhängigen optimalen Multiplikator  
 $r_{\text{opt}}$ . Falls der gewählte Wert von  $r$  geringfügig kleiner als das Optimum ist,  
enthält das Produkt  $p \cdot r$  immer noch genügend viele führende Einsen, um die  
25 Division einfach gestalten zu können. Mit hoher Wahrscheinlichkeit ist die  
Zahl  $d$  teilerfremd zu mindestens einem der Werte  $\phi(r_{\text{opt}}^{-i})$ , wobei  $i = 1, \dots, k$ ,  
wobei  $k$  eine von der Implementation abhängige kleine Zahl ist.

- 11 -

Wenn dies nicht der Fall ist, ersetze man  $r$  durch  $2^i \cdot r$ , wobei  $2^i$  eine von der Implementierung abhängige geeignete Zweierpotenz ist.

5 Dieselben Substitutionen sind entsprechend auch auf den zweiten Primfaktor  $q$  anwendbar. Da die Multiplikatoren  $r$  (für  $p$ ) und  $s$  (für  $q$ ) unabhängig voneinander gewählt werden können, ist für den Multiplikator  $s$  ebenfalls eine entsprechende Wahl möglich.

## Patentansprüche

### 1. Kryptographisches Verfahren,

a) mit mindestens einem eine modulare Exponentiation E

$$E = x^d \pmod{p \cdot q}$$

5       enthaltenden Rechenschritt mit einem ersten Primfaktor p, einem zweiten Primfaktor q, einem Exponenten d und einer Basis x, wobei

b) zur Durchführung der modularen Exponentiation zwei natürliche Zahlen r und s gewählt werden mit der Bedingung, daß d teilerfremd ist zu  $\phi(\text{kgV}(r,s))$  und wobei die folgenden Rechenschritte

10       durchgeführt werden:

$$x_1 = x \pmod{p \cdot r}$$

$$x_2 = x \pmod{q \cdot s}$$

$$d_1 = d \pmod{\phi(p \cdot r)}$$

$$d_2 = d \pmod{\phi(q \cdot s)}$$

15        $z_1 = x_1^{d_1} \pmod{p \cdot r}$

$$z_2 = x_2^{d_2} \pmod{q \cdot s},$$

und wobei  $\phi(\cdot)$  die Euler'sche Funktion und  $\text{kgV}(r,s)$  das kleinste gemeinsame Vielfache von r und s darstellt,

c) anschließend nach dem Chinesischen Restwertsatz aus  $z_1$  und  $z_2$  eine

20       Zahl z berechnet wird mit  $z = z_1 \pmod{p \cdot r}$  ;  $z = z_2 \pmod{q \cdot s}$  ;

d) das Ergebnis E der Exponentiation durch Reduktion von z

modulo  $p \cdot q$  berechnet wird

e) die vorher berechnete Zahl z und damit das Ergebnis E in einem Prüfschritt auf Rechenfehler geprüft wird,

25       f) der Prüfschritt folgende Rechenoperationen beinhaltet:

- f1) Berechnen der kleinstmöglichen natürlichen Zahl  $e$  mit der Eigenschaft  $e \cdot d = 1 \pmod{\phi(\text{kgV}(r,s))}$  mit Hilfe des erweiterten Euklids'schen Algorithmus
- f2) Berechnen des Wertes  $C = z^e \pmod{\text{kgV}(r,s)}$
- 5 f3) Vergleich der Werte  $x$  und  $C$  modulo  $\text{kgV}(r,s)$ , wobei das Ergebnis der modularen Exponentiation  $E$  als fehlerhaft verworfen wird, wenn  $x \neq C \pmod{\text{kgV}(r,s)}$ .

## 2. Kryptographisches Verfahren,

- 10 a) mit mindestens einer eine modulare Exponentiation  $E$   
 $E = x^d \pmod{p \cdot q}$   
 enthaltenden Rechenschritt mit einem ersten Primfaktor  $p$ , einem zweiten Primfaktor  $q$ , einem Exponenten  $d$  und einer Basis  $x$ , wobei
- b) zur Durchführung der modularen Exponentiation zwei natürliche  
 15 Zahlen  $r$  und  $s$ , sowie zwei Zahlen  $b_1$  und  $b_2$  im Intervall  $[1, \dots, r-1]$   
 bzw.  $[1, \dots, s-1]$  und teilerfremd zu  $r$  bzw.  $s$  gewählt werden, und wobei  $b_1$  und  $b_2$  die Bedingung  $b_1 = b_2 \pmod{\text{ggT}(r,s)}$  erfüllen, wobei  $\text{ggT}(r,s)$  den größten gemeinsamen Teiler von  $r$  und  $s$  bezeichnet,
- c) mit Hilfe der beiden Zahlen  $b_1$  und  $b_2$  nach dem Chinesischen Rest-  
 20 wertsatz Werte  $x_1$  und  $x_2$  berechnet werden, die die folgenden Bedingungen erfüllen:

$$x_1 = x \pmod{p}, \quad x_1 = b_1 \pmod{r}$$

$$x_2 = x \pmod{q}, \quad x_2 = b_2 \pmod{s}$$

und anschließend folgende Rechenschritte durchgeführt werden:

- 25  $d_1 = d \pmod{\phi(p)}$   
 $d_2 = d \pmod{\phi(q)}$   
 $z_1 = x_1^{d_1} \pmod{p \cdot r}$   
 $z_2 = x_2^{d_2} \pmod{q \cdot s}$

und  $\phi(\cdot)$  die Euler'sche Funktion und  $\text{kgV}(r,s)$  das kleinste gemeinsame Vielfache von  $r$  und  $s$  darstellt,

d) anschließend nach dem Chinesischen Restwertsatz aus  $z_1$  und  $z_2$  eine Zahl  $z$  berechnet wird mit  $z = z_1 \pmod{p \cdot r}$  ;  $z = z_2 \pmod{q \cdot s}$  ;

5 e) das Ergebnis  $E$  der Exponentiation durch Reduktion von  $z$  modulo  $p \cdot q$  berechnet wird

f) die vorher berechnete Zahl  $z$  (und damit automatisch auch das Ergebnis  $E$ ) in einem Prüfschritt auf Rechenfehler geprüft wird,

g) der Prüfschritt folgende Rechenoperationen beinhaltet:

10 g1) Berechnen der Zahlen

$$C_1 = b_1^{d_1} \pmod{r}$$

$$C_2 = b_2^{d_2} \pmod{s}$$

wobei  $d_1$  und  $d_2$  vor der Durchführung der modularen Exponentiation modulo  $\phi(r)$  bzw.  $\phi(s)$  reduziert werden

15 g2) Vergleich der Werte  $z_1$  und  $C_1$  modulo  $r$  sowie  $z_2$  und  $C_2$  modulo  $s$ , wobei das Ergebnis der modularen Exponentiation  $E$  als fehlerhaft verworfen wird, wenn  $C_1 \neq z_1 \pmod{r}$  oder  $C_2 \neq z_2 \pmod{s}$  gilt.

20 3. Kryptographisches Verfahren nach Anspruch 2, dadurch gekennzeichnet, daß die Zahlen  $r$  und  $s$  ungerade sind.

4. Kryptographisches Verfahren nach Anspruch 1 bis 3, dadurch gekennzeichnet, daß die Zahlen  $r$  und  $s$  im Bereich  $[0, 2^k-1]$  mit  $16 \leq k \leq 32$  ausgewählt werden.

25 5. Kryptographisches Verfahren nach Anspruch 1 bis 4, dadurch gekennzeichnet, daß mindestens eine der Zahlen  $r$  und  $s$  so gewählt wird, daß die



Binärdarstellung des Produktes  $p \cdot r$  beziehungsweise  $q \cdot s$  möglichst viele führende Einsen enthält.

6. Kryptographisches Verfahren nach einem der Ansprüche 1 bis 5, **dadurch gekennzeichnet**, daß beide Zahlen  $r$  und  $s$  so gewählt werden, daß die Binärdarstellung des Produktes  $p \cdot r$  und des Produktes  $q \cdot s$  möglichst viele führende Einsen enthalten.

7. Kryptographisches Verfahren nach einem der Ansprüche 5 oder 6, **dadurch gekennzeichnet**, daß

- a) in einem ersten Teilschritt zunächst für mindestens eine der Zahlen  $r$  und  $s$  eine entsprechende optimale Zahl  $r_{opt}$  beziehungsweise  $s_{opt}$  ohne Beschränkung durch die Bedingung, gemäß der  $d$  teilerfremd zu  $\phi(\text{kgV}(r,s))$  ist, ausgewählt wird, und
- b) in einem zweiten Teilschritt jeweils ein benachbarter Wert  $r = r_{opt} - i$  beziehungsweise  $s = s_{opt} - i$ ,  $i = 0, 1, \dots, k$ , ausgewählt wird, so daß  $d$  teilerfremd zu  $\phi(\text{kgV}(r,s))$  ist.

8. Kryptographisches Verfahren nach einem der Ansprüche 5 oder 6, **dadurch gekennzeichnet**, daß

- a) in einem ersten Teilschritt für jede der Zahlen  $r$  und  $s$  eine entsprechende optimale Zahl  $r_{opt}$  beziehungsweise  $s_{opt}$  ohne Beschränkung durch die Bedingung, gemäß der  $d$  teilerfremd zu  $\phi(\text{kgV}(r,s))$  ist, ausgewählt wird, und
- b) in einem zweiten Teilschritt jeweils ein Wert  $r = 2^l \cdot r_{opt}$  beziehungsweise  $s = 2^l \cdot s_{opt}$ ,  $l = 0, 1, \dots, j$ , ausgewählt wird, so daß  $d$  teilerfremd zu  $\phi(\text{kgV}(r,s))$  ist.

9. Kryptographisches Verfahren nach einem der Ansprüche 5 oder 6, **dadurch gekennzeichnet**, daß

- a) in einem ersten Teilschritt mindestens eine der Zahlen  $r_{\text{opt}}$  und  $s_{\text{opt}}$  zunächst ohne Beschränkung durch die Bedingung, gemäß der  $d$  teilerfremd zu  $\phi(\text{kgV}(r,s))$  ist, ausgewählt wird,
- b) in einem zweiten Teilschritt jeweils ein benachbarter Wert  $r = r_{\text{opt}} - i$  beziehungsweise  $s = s_{\text{opt}} - i$ ,  $i = 0, 1, \dots, k$ , ausgewählt wird, so daß  $d$  teilerfremd zu  $\phi(\text{kgV}(r,s))$  ist, falls ein solcher Wert für  $i = 0, 1, \dots, k$  existiert, und
- c) in einem dritten Teilschritt jeweils ein Wert  $r = 2^l \cdot r_{\text{opt}}$  beziehungsweise  $s = 2^l \cdot s_{\text{opt}}$ ,  $i = 0, 1, \dots, j$ , ausgewählt wird, so daß  $d$  teilerfremd zu  $\phi(\text{kgV}(r,s))$  ist, falls im zweiten Teilschritt kein Wert ausgewählt worden ist.

10. Kryptographisches Verfahren nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet**, daß es das RSA-Verfahren beinhaltet.

11. Kryptographisches Verfahren nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet**, daß es das Rabin'sche-Signaturen-Verfahren beinhaltet.

12. Kryptographisches Verfahren nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet**, daß es das Fiat-Shamir'sche Identifikationsschema-Verfahren beinhaltet.

13. Kryptographische Vorrichtung,

a) mit mindestens einer Exponentiationseinrichtung, die einen eine modulare Exponentiation  $E$

$$E = x^d \pmod{p \cdot q}$$

enthaltenden Rechenschritt mit einem ersten Primfaktor  $p$ , einem zweiten Primfaktor  $q$ , einem Exponenten  $d$  und einer Basis  $x$  ausführt, wobei

- b) zur Durchführung der modularen Exponentiation zwei natürliche Zahlen  $r$  und  $s$  gewählt werden mit der Bedingung, daß  $d$  teilerfremd ist zu  $\phi(\text{kgV}(r,s))$  und wobei die folgenden Rechenschritte durchgeführt werden:

$$\begin{aligned} x_1 &= x \pmod{p \cdot r} \\ x_2 &= x \pmod{q \cdot s} \\ d_1 &= d \pmod{\phi(p \cdot r)} \\ d_2 &= d \pmod{\phi(q \cdot s)} \\ z_1 &= x_1^{d_1} \pmod{p \cdot r} \\ z_2 &= x_2^{d_2} \pmod{q \cdot s}, \end{aligned}$$

und  $\phi(\cdot)$  die Euler'sche Funktion und  $\text{kgV}(r,s)$  das kleinste gemeinsame Vielfache von  $r$  und  $s$  darstellt,

- c) anschließend nach dem Chinesischen Restwertsatz aus  $z_1$  und  $z_2$  eine Zahl  $z$  berechnet wird mit  $z = z_1 \pmod{p \cdot r}$  ;  $z = z_2 \pmod{q \cdot s}$  ;

d) das Ergebnis  $E$  der Exponentiation durch Reduktion von  $z$  modulo  $p \cdot q$  berechnet wird

- e) die vorher berechnete Zahl  $z$  (und damit automatisch auch das Ergebnis  $E$ ) in einem Prüfschritt auf Rechenfehler geprüft wird,

f) der Prüfschritt folgende Rechenoperationen beinhaltet:

- f1) Berechnen der kleinstmöglichen natürlichen Zahl  $e$  mit der Eigenschaft  $e \cdot d = 1 \pmod{\phi(\text{kgV}(r,s))}$  mit Hilfe des erweiterten Euklid'schen Algorithmus

f2) Berechnen des Wertes  $C = z^e \pmod{\text{kgV}(r,s)}$

f3) Vergleich der Werte  $x$  und  $C$  modulo  $\text{kgV}(r,s)$ , wobei das Ergebnis der modularen Exponentiation  $E$  als fehlerhaft verworfen wird, wenn  $x \neq C \pmod{\text{kgV}(r,s)}$ .

5 14. . Kryptographische Vorrichtung,

a) mit mindestens einer Exponentiationseinrichtung, die einen eine modulare Exponentiation  $E$

$$E = x^d \pmod{p \cdot q}$$

enthaltenden Rechenschritt mit einem ersten Primfaktor  $p$ , einem

10 zweiten Primfaktor  $q$ , einem Exponenten  $d$  und einer Basis  $x$  ausführt, wobei

b) zur Durchführung der modularen Exponentiation zwei natürliche Zahlen  $r$  und  $s$ , sowie zwei Zahlen  $b_1$  und  $b_2$  im Intervall  $[1, \dots, r-1]$

15 bzw.  $[1, \dots, s-1]$  und teilerfremd zu  $r$  bzw.  $s$  gewählt werden, und wobei  $b_1$  und  $b_2$  die Bedingung  $b_1 = b_2 \pmod{\text{ggT}(r,s)}$  erfüllen, wobei  $\text{ggT}(r,s)$  den größten gemeinsamen Teiler von  $r$  und  $s$  bezeichnet,

c) mit Hilfe der beiden Zahlen  $b_1$  und  $b_2$  nach dem Chinesischen Restwertsatz Werte  $x_1$  und  $x_2$  berechnet werden, die die folgenden Bedingungen erfüllen:

20 
$$x_1 = x \pmod{p}, \quad x_1 = b_1 \pmod{r}$$

$$x_2 = x \pmod{q}, \quad x_2 = b_2 \pmod{s}$$

und anschließend folgende Rechenschritte durchgeführt werden:

$$d_1 = d \pmod{\phi(p)}$$

$$d_2 = d \pmod{\phi(q)}$$

25 
$$z_1 = x_1^{d_1} \pmod{p \cdot r}$$

$$z_2 = x_2^{d_2} \pmod{q \cdot s}$$

und wobei  $\phi(\cdot)$  die Euler'sche Funktion und  $\text{kgV}(r,s)$  das kleinste gemeinsame Vielfache von  $r$  und  $s$  darstellt,

- d) anschließend nach dem Chinesischen Restwertsatz aus  $z_1$  und  $z_2$  eine Zahl  $z$  berechnet wird mit  $z = z_1 \pmod{p \cdot r}$  ;  $z = z_2 \pmod{q \cdot s}$  ;
- e) das Ergebnis  $E$  der Exponentiation durch Reduktion von  $z$  modulo  $p \cdot q$  berechnet wird
- 5 f) die vorher berechnete Zahl  $z$  (und damit automatisch auch das Ergebnis  $E$ ) in einem Prüfschritt auf Rechenfehler geprüft wird,
- g) der Prüfschritt folgende Rechenoperationen beinhaltet:
- g1) Berechnen der Zahlen
- $$C_1 = b_1^{d_1} \pmod{r}$$
- $$C_2 = b_2^{d_2} \pmod{s}$$
- 10 wobei  $d_1$  und  $d_2$  vor der Durchführung der modularen Exponentiation modulo  $\phi(r)$  bzw.  $\phi(s)$  reduziert werden,
- g2) Vergleich der Werte  $z_1$  und  $C_1$  modulo  $r$  sowie  $z_2$  und  $C_2$  modulo  $s$ , wobei das Ergebnis der modularen Exponentiation  $E$  als fehlerhaft
- 15 verworfen wird, wenn  $C_1 \neq z_1 \pmod{r}$  oder  $C_2 \neq z_2 \pmod{s}$  gilt.

15. Kryptographische Vorrichtung nach Anspruch 14, **dadurch gekennzeichnet**, daß die Zahlen  $r$  und  $s$  ungerade sind.

- 20 16. Kryptographische Vorrichtung nach Anspruch 13 bis 15, **dadurch gekennzeichnet**, daß die Zahlen  $r$  und  $s$  im Bereich  $[0, 2^k - 1]$  mit  $16 \leq k \leq 32$  ausgewählt werden.

- 25 17. Kryptographische Vorrichtung nach Anspruch 13 bis 16, **dadurch gekennzeichnet**, daß mindestens eine der Zahlen  $r$  und  $s$  so gewählt wird, daß die Binärdarstellung des Produktes  $p \cdot r$  beziehungsweise  $q \cdot s$  möglichst viele führende Einsen enthält.

18. Kryptographische Vorrichtung nach einem der Ansprüche 13 bis 17, **dadurch gekennzeichnet**, daß beide Zahlen  $r$  und  $s$  so gewählt werden, daß die Binärdarstellung des Produktes  $p \cdot r$  und des Produktes  $q \cdot s$  möglichst viele führende Einsen enthalten.

5

19. Kryptographische Vorrichtung nach einem der Ansprüche 17 oder 18, **dadurch gekennzeichnet**, daß

- a) in einem ersten Teilschritt zunächst für mindestens eine der Zahlen  $r$  und  $s$  eine entsprechende optimale Zahl  $r_{\text{opt}}$  beziehungsweise  $s_{\text{opt}}$  ohne Beschränkung durch die Bedingung, gemäß der  $d$  teilerfremd zu  $\phi(\text{kgV}(r,s))$  ist, ausgewählt wird, und
- b) in einem zweiten Teilschritt jeweils ein benachbarter Wert  $r = r_{\text{opt}} - i$  beziehungsweise  $s = s_{\text{opt}} - i$ ,  $i = 0, 1, \dots, k$ , ausgewählt wird, so daß  $d$  teilerfremd zu  $\phi(\text{kgV}(r,s))$  ist.

15

20. Kryptographische Vorrichtung nach einem der Ansprüche 17 oder 18, **dadurch gekennzeichnet**, daß

- a) in einem ersten Teilschritt für jede der Zahlen  $r$  und  $s$  eine entsprechende optimale Zahl  $r_{\text{opt}}$  beziehungsweise  $s_{\text{opt}}$  ohne Beschränkung durch die Bedingung, gemäß der  $d$  teilerfremd zu  $\phi(\text{kgV}(r,s))$  ist, ausgewählt wird, und
- b) in einem zweiten Teilschritt jeweils ein Wert  $r = 2^l \cdot r_{\text{opt}}$  beziehungsweise  $s = 2^l \cdot s_{\text{opt}}$ ,  $l = 0, 1, \dots, j$ , ausgewählt wird, so daß  $d$  teilerfremd zu  $\phi(\text{kgV}(r,s))$  ist.

25

21. Kryptographische Vorrichtung nach einem der Ansprüche 17 oder 18, **dadurch gekennzeichnet**, daß

- a) in einem ersten Teilschritt mindestens eine der Zahlen  $r_{\text{opt}}$  und  $s_{\text{opt}}$  zunächst ohne Beschränkung durch die Bedingung, gemäß der  $d$  teilerfremd zu  $\phi(\text{kgV}(r,s))$  ist, ausgewählt wird,
- b) in einem zweiten Teilschritt jeweils ein benachbarter Wert  $r = r_{\text{opt}} - i$  beziehungsweise  $s = s_{\text{opt}} - i$ ,  $i = 0, 1, \dots, k$ , ausgewählt wird, so daß  $d$  teilerfremd zu  $\phi(\text{kgV}(r,s))$  ist, falls ein solcher Wert für  $i = 0, 1, \dots, k$  existiert, und
- c) in einem dritten Teilschritt jeweils ein Wert  $r = 2^l \cdot r_{\text{opt}}$  beziehungsweise  $s = 2^l \cdot s_{\text{opt}}$ ,  $l = 0, 1, \dots, j$ , ausgewählt wird, so daß  $d$  teilerfremd zu  $\phi(\text{kgV}(r,s))$  ist, falls im zweiten Teilschritt kein Wert ausgewählt worden ist.

22. Kryptographische Vorrichtung nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet**, daß es das RSA-Verfahren beinhaltet.
- 15 23. Kryptographische Vorrichtung nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet**, daß es das Rabin'sche-Signaturen-Verfahren beinhaltet.
- 20 24. Kryptographische Vorrichtung nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet**, daß es das Fiat-Shamir'sche Identifikationsschema-Verfahren beinhaltet.

(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 Classification<sup>7</sup>: 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). ANDER-  
SON, Allan, D.; 11158 Bertha Place, Cerritos, CA 90703

(US). GODDING, Patrick, N.; 22665 Shady Grove Cir-  
cle, Lake Forest, CA 92630 (US). PUNT, Maarten, G.;  
24942 Paseo Arboleda, Lake Forest, CA 92630 (US). SO-  
TOODEH, Mehdi; 17 Paloma Drive, Mission Viejo, CA  
92692 (US).

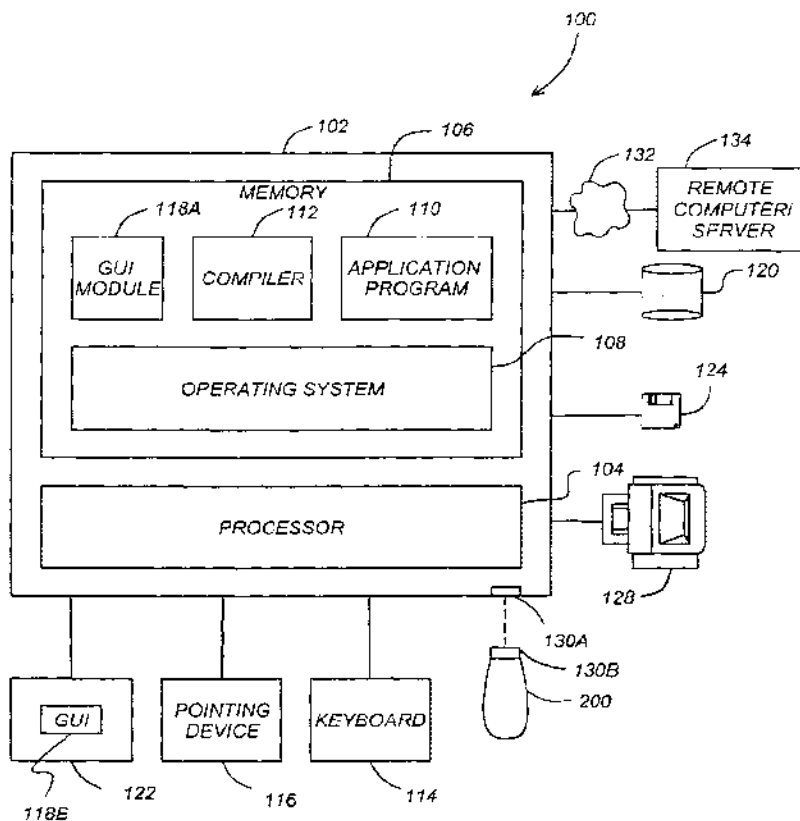
(74) Agents: SMITH, Samuel, Leonard et al.; J.A. Kemp &  
Co., 14 South Square, Gray's Inn, London WC1R 5JJ (GB).

(81) Designated States (national): AE, AG, AI, 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 (GI, 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 EM-  
ULATOR



(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 (AE, 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).

*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.*

**Published:**

*without international search report and to be republished upon receipt of that report*

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  
5 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  
10 by Shawn D. Abbott, Bahram 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

15 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.

20 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  
25 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.

25

#### 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)

15

#### 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;

20 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

25 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  
5 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  
10 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  
15 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  
20 112 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  
25 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,  
5 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  
10 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  
15 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  
20 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,  
25 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  
5 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  
10 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  
15 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  
20 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  
25 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.

5           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  
10   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  
15   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.

20           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  
25   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

5 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  
10 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  
15 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  
20 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  
25 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)

5

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 unpacked 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-  
5 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  
10 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  
15 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  
20 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  
25 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 (TA<sub>i</sub>, TB<sub>i</sub>, TC<sub>i</sub>, and TD<sub>i</sub>), historical characters (T<sub>1</sub>, T<sub>2</sub>, . . . , 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.

5           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  
10 130. 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  
15 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  
20 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

5

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

5

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 releasably 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

10

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;  
5 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  
10 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  
15 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  
20 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);
  - 5 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
  - 10 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.
- 15 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
  - 20 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
  - 25 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;

5 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

10 (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;

15 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);

20 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  
5 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);  
10 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  
15 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:  
20 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).

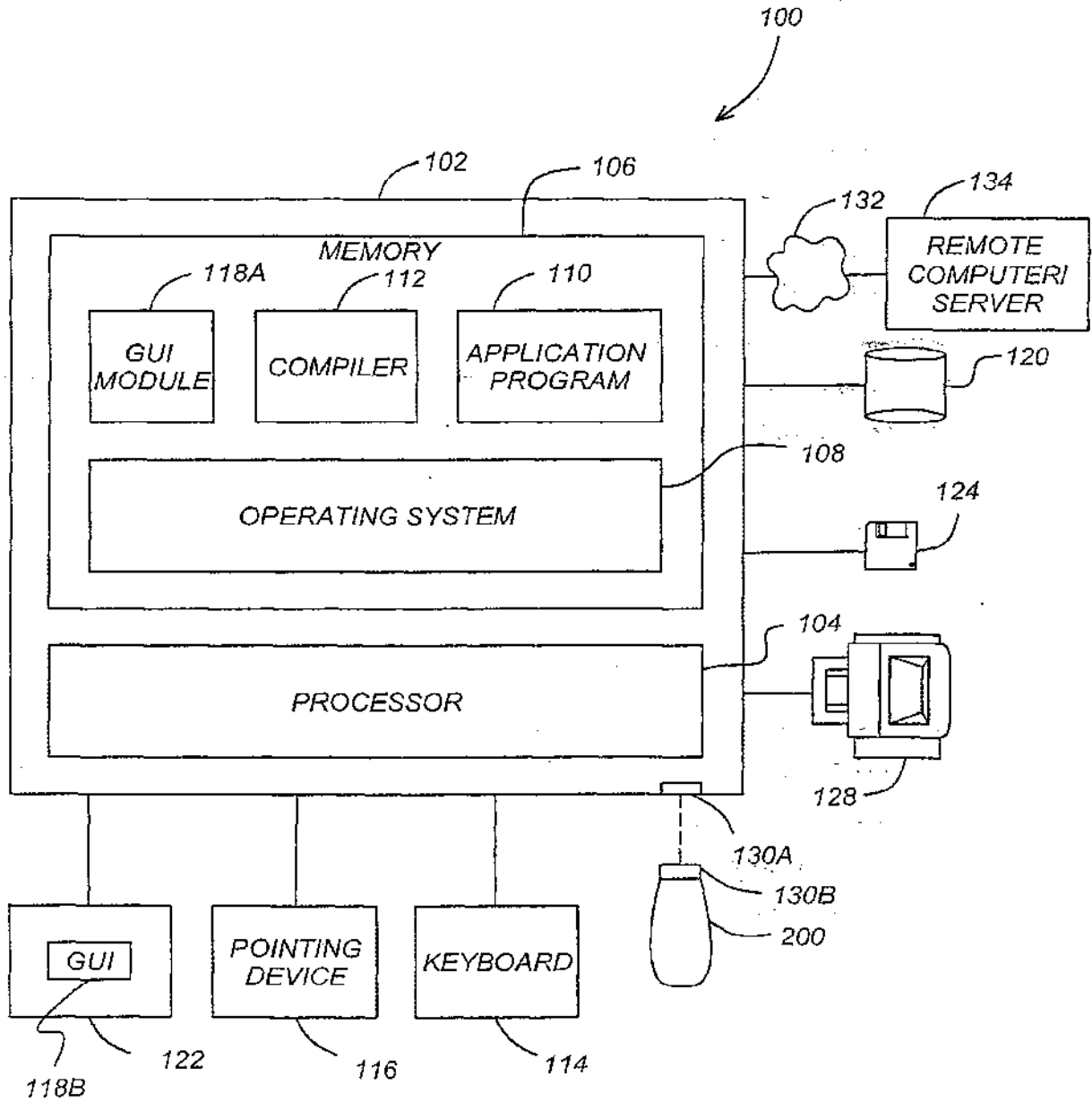


FIG. 1

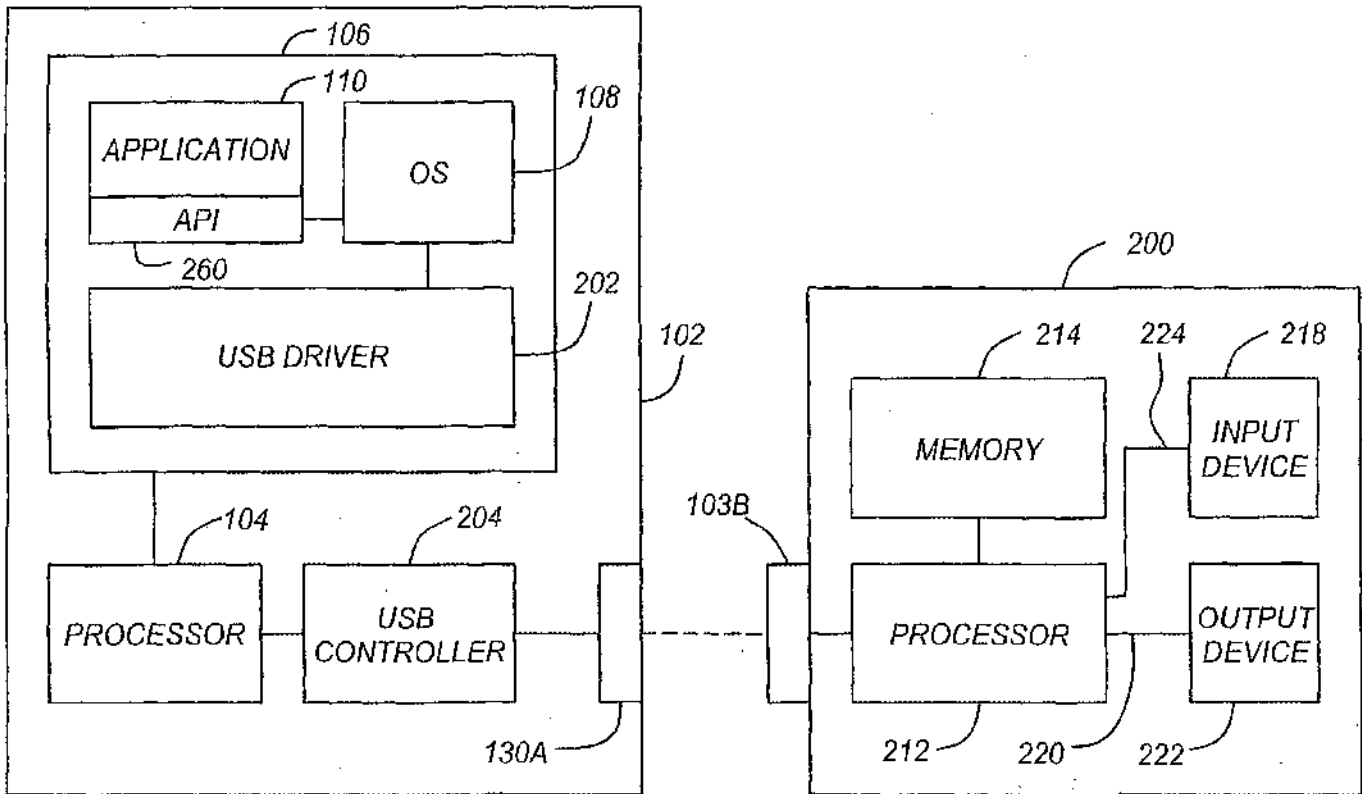


FIG. 2

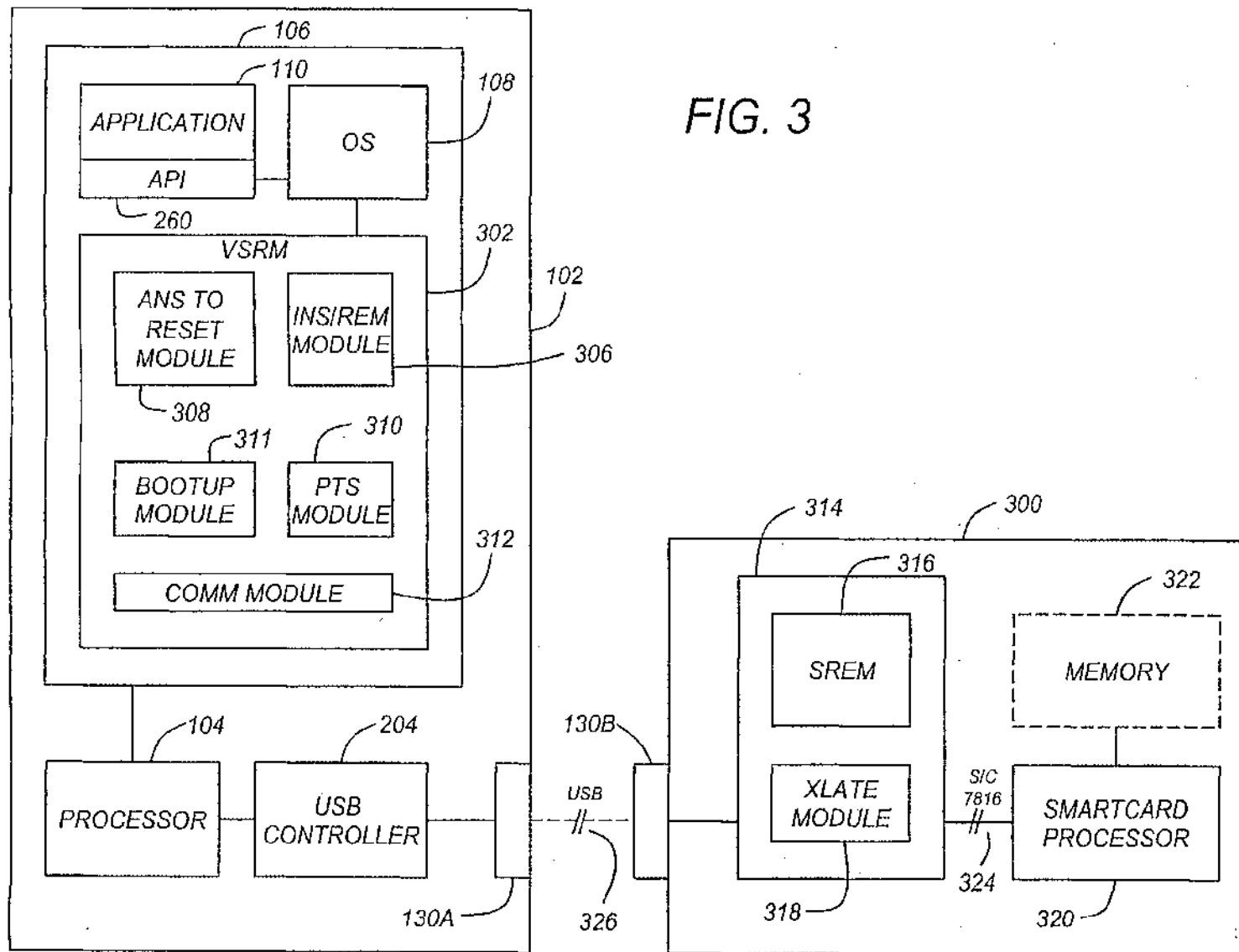


FIG. 3

3/7

4/7

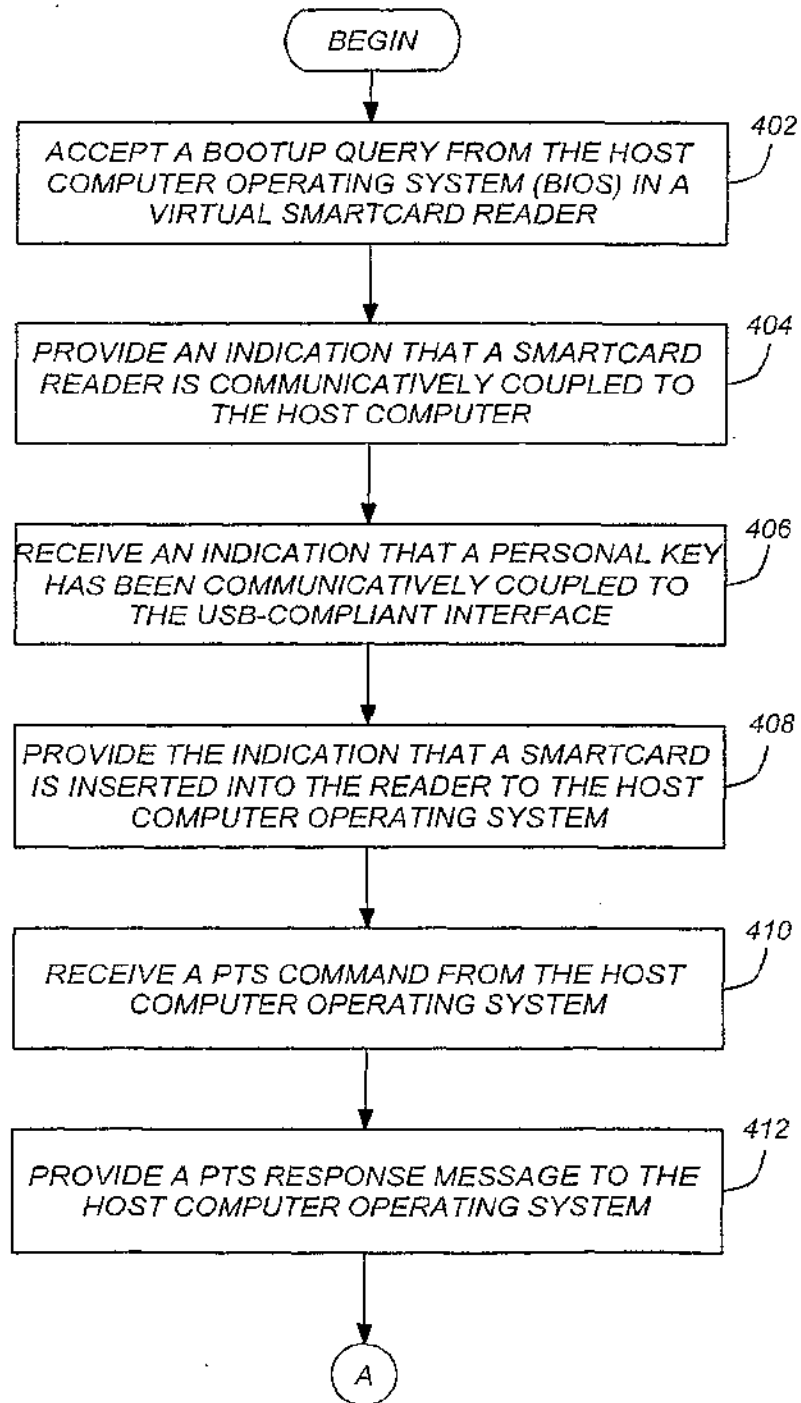


FIG. 4A

5/7

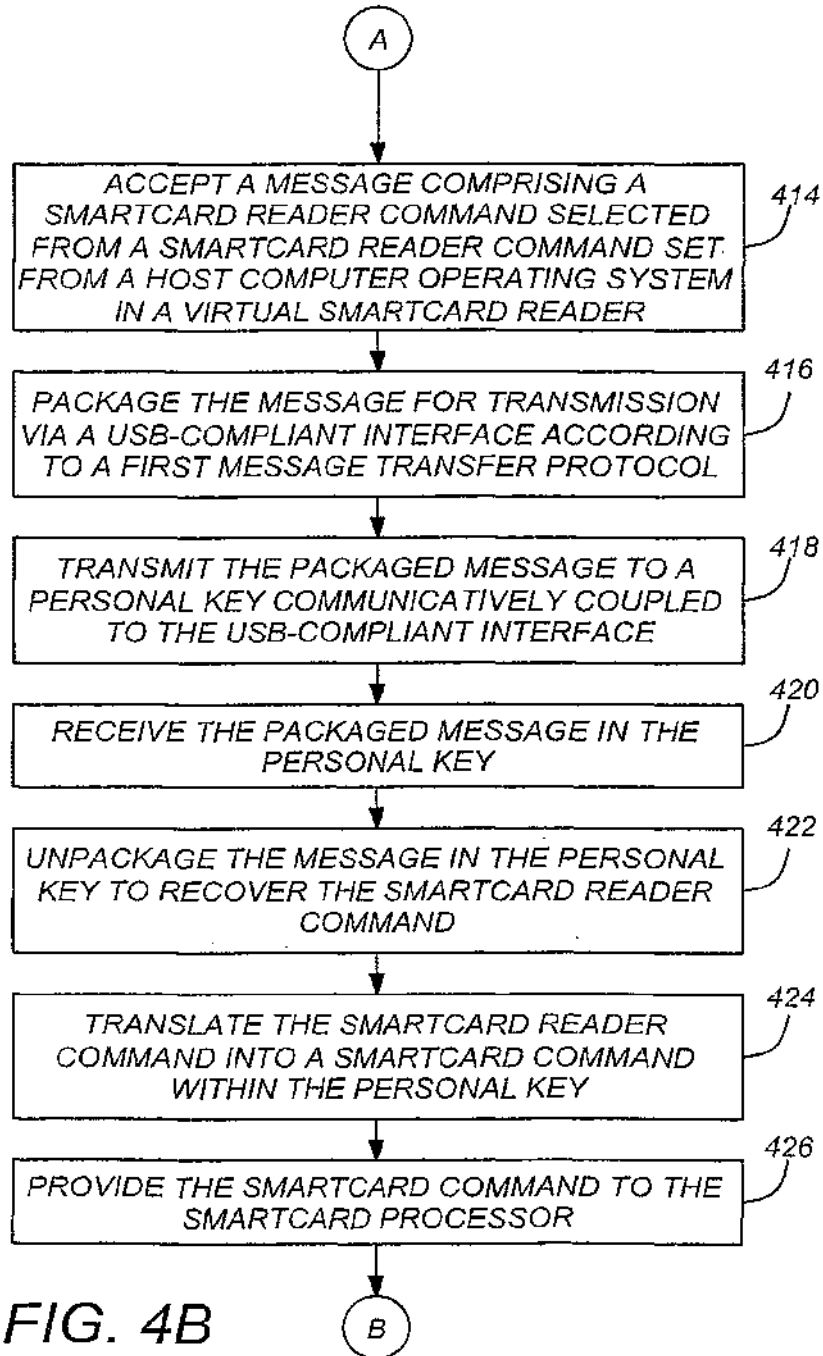


FIG. 4B

6/7

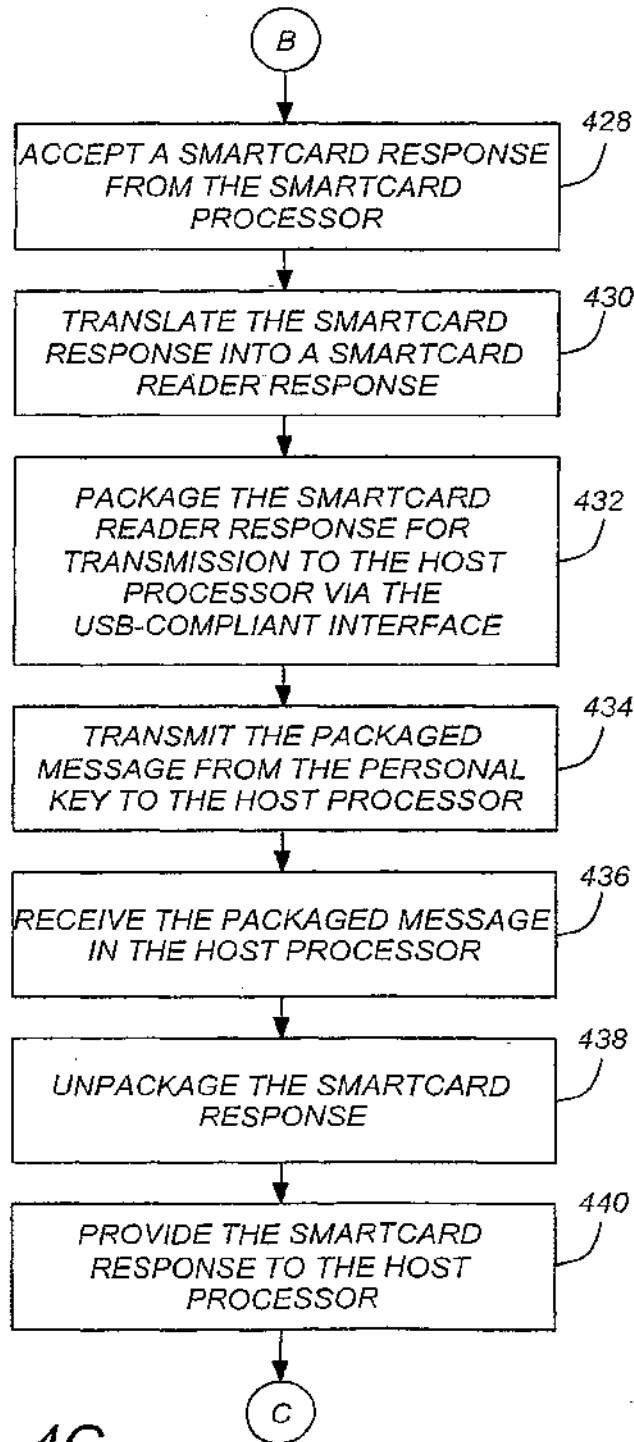


FIG. 4C

7/7

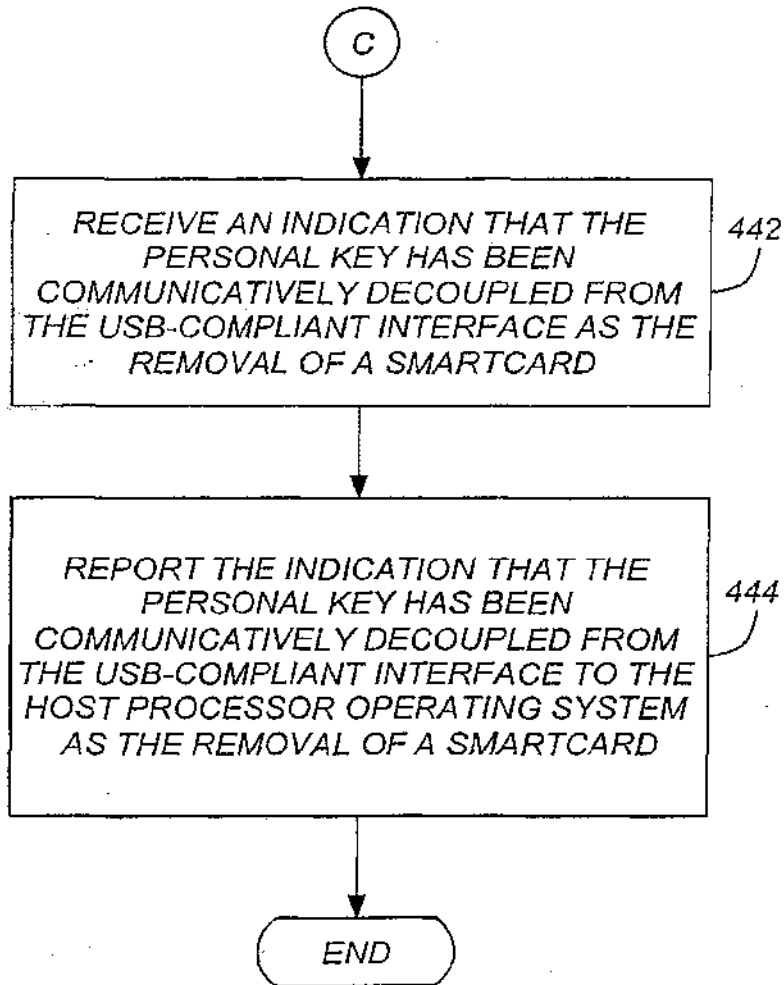


FIG. 4D



(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
20 February 2003 (20.02.2003)

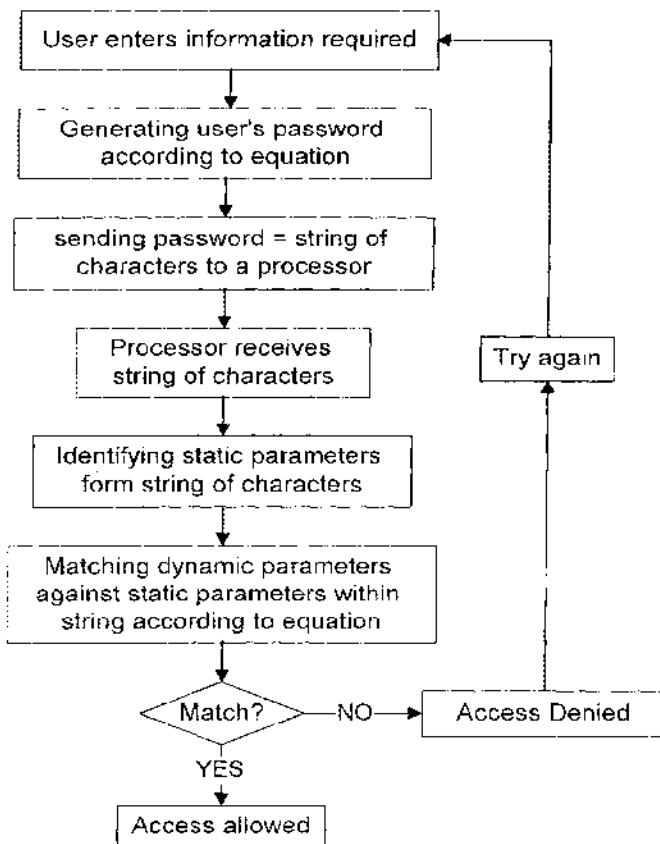
PCT

(10) International Publication Number  
**WO 03/014887 A2**

- (51) International Patent Classification<sup>7</sup>: **G06F 1/00**
- (21) International Application Number: PCT/EP02/08069
- (22) International Filing Date: 18 July 2002 (18.07.2002)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:  
09/924,502 9 August 2001 (09.08.2001) US
- (71) Applicant: **ACTIVCARD IRELAND, LIMITED**  
[IE/IE]: -, 30 Herbert Street, Dublin 2 (IE).
- (72) Inventor: **HILLHOUSE, Robert, D.**; Unit 4B, 120 Holland Avenue, Ottawa, Ontario K1Y0X6 (CA).
- (74) Agent: **CABINET JP COLAS**; -, 37 avenue Franklin D. Roosevelt, F-75008 Paris (FR).
- (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, OM, PH, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN, YU, ZA, ZM, ZW.
- (84) Designated States (*regional*): ARIPO patent (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD FOR SUPPORTING DYNAMIC PASSWORD



(57) Abstract: A method of generating dynamic password is disclosed. A method of generating a dynamic password comprising the steps of providing a plurality of variable parameters, each parameter from the plurality of variable parameters being variable upon predetermined criteria; providing a plurality of predetermined static parameters; and processing at least some of the plurality of variable parameters and of the predetermined static parameters according to a dynamic password generating equation manipulating at least some of the plurality of variable parameters and of the predetermined static parameters resulting in an ordered sequence of dynamic and static parameters.



WO 03/014887 A2



**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.*

## Method for Supporting Dynamic Password

[001] The present invention relates to a method of generating passwords and more particularly to a method of generating a password that changes as a function of various parameters making the password dynamic.

### 5 Background of the Invention

[002] Security is fast becoming an important issue. It has always been an issue for everybody to protect his belongings. It is also well known that with the proliferation of computers and computer networks into all aspects of business and daily life - financial, medical, education, government, and communications - the concern over secure file  
10 access is growing. Using passwords is a common method of providing security. Password protection and/or combination type locks are employed for computer network security, automatic teller machines, telephone banking, calling cards, telephone answering services, houses, and safes. These systems generally require the knowledge of an entry code that has been selected by a user or has been preset.

15 [003] Preset codes are often forgotten, as users have no reliable method of remembering them. Writing down the codes and storing them in close proximity to an access control device (i.e., the combination lock) results in a secure access control system with a very insecure code. Alternatively, the nuisance of trying several code variations renders the access control system more of a problem than a solution.

20 [004] It is well known that a user determines a meaningful password, in the form of, for example, the name of their dog, the birth date of their child or an election year of the favorite candidate. This type of password is easily compromised with investigation. Conversely, a computer can randomly associate a password with a user, but this type of password is meaningless to the user and as such difficult to memorize.  
25 Consequently, the former method, which is simple, is insecure and the latter method, which is more secure, is difficult to use and often leads to a user writing their password next to their computer, thereby making the system insecure.

[005] The multiplicity of protected systems encountered in the daily life of an individual renders the use of password particularly inconvenient, because a user has to  
30 remember a password for each accessible system. For example, the user must remember passwords for accessing network, database, E-mail, bank machine, personal

voice mails at home and at work, etc. The plurality of the systems wherein a password is needed favors a single simple password for all systems. In addition, a skilled person may find a predetermined password given sufficient time, rendering the system insecure. In more sophisticated theft situations, "Trojan horse" type viruses can be used to capture a user ID number and password that have been entered at a keyboard or  
5 across a network connection. That is, the user thinks he is logging on as usual, but the dialogue box in which the data is entered is really a look-alike window that is capturing his keystrokes.

[006] To secure access to a network, a further system was developed that relies on a user's personal information. A user requesting access to the network is prompted to  
10 answer a series of questions regarding his private life displayed on a computer screen. Such questions might be related to a relative's date of birth, a bone that was broken during childhood, a year of his first car accident, insurance company, address in January 1994, name of his first girlfriend, etc. The computer checks the validity of the answers  
15 before allowing access to the user. A computer is programmed with pertinent questions to ask a user and answers associated therewith, and when the system is initialised, the user enters the answers a first time, they are stored in a memory of the system, and are associated with the user identity. The time taken to answer all the questions prior to gaining access to the system is burdensome. It is evident that a major inconvenient  
20 with such a system is that a skilled person can find enough information of a personal nature relating to a user for answering properly the questions, and as such render the security ineffectual.

### **Object of the Invention**

25 [007] To overcome such disadvantages, it is an object of this invention to provide a method for rendering a computer system access more secure.

[008] It is another object of this invention to provide a method for generating dynamic password.

[009] It is a further object of this invention to provide a method for generating a  
30 dynamic password dependent on various dynamic parameters.

**Summary of the Invention**

[0010] In accordance with a preferred embodiment of the present invention, there is provided a method of password verification comprising the steps of:

5 providing a process for transforming at least a variable parameter into an ordered string of characters, wherein the process sometimes results in different ordered strings of characters for a same variable parameter;

providing at least a variable parameter as a known password;

determining from data available to an individual and from the known password a static string;

10 providing the determined static string as a password for verification;

verifying the static string to determine that it is an accurate transformation of the at least a variable parameter according to the provided process and when the determination is that the transformation is accurate, providing an indication that the password is verified.

15 [0011] In accordance with another preferred embodiment of the present invention, there is provided a method of changing dynamic passwords comprising the steps of:

providing a string of characters, the string including indications of at least a parameter from a plurality of parameters, the at least a parameter being a variable parameter variable upon predetermined criteria;

20 receiving the provided string of characters; and,

storing data based on the known password, the data sufficient for verifying provided passwords to determine their accuracy.

[0012] Advantageously, the invention provides a method of verifying a dynamic password comprising the steps of:

25 receiving a password comprising a string of characters wherein the characters are sequenced according to a predetermined sequence of variable parameters and static parameters;

identifying static parameters within the string of characters;

determining dynamic parameter values related to the dynamic parameters in accordance with the predetermined sequence ;

comparing static parameters received within the string of characters with previously stored static parameters and the received dynamic parameter within the determined dynamic parameters to determine a first comparison result;

wherein upon both the first comparison result being indicative of a match, the dynamic password is validated.

Further advantageously, the invention provides a method of generating a dynamic password comprising the steps of:

providing a process for transforming at least a variable parameter into an ordered string of characters, wherein the process sometimes results in different ordered strings of characters for a same variable parameter; and,

providing at least a variable parameter as a password, the provided variable parameter provided by an individual via a data entry device.

#### **Brief description of the drawings**

[0013] Exemplary embodiments of the invention will now be described in conjunction with the following drawings, in which:

[0014] Fig. 1 is a computer screen display of a password dialog box;

[0015] Fig. 1a is an example of a filled password dialog box on a computer screen display;

[0016] Fig. 2 is a flow diagram of a method of evaluating a dynamic password generated according to the present invention;

[0017] Fig. 3 is an illustration of a computer screen displaying some possible images incorporated in the password;

#### **Detailed Description of the Invention**

[0018] In many large companies, the computer system is organized as a network to reduce the cost of purchasing and installing software on all the stations existing in the company. A main advantage of using a network is to facilitate data accessibility to each

employee. However, it is necessary to limit access of a company's network to the company's employees. As such, Fig. 1 is an example of a screen display prompting an employee to enter a login identity and an associated password to allow the employee to access the network. An example of a filled dialog box is shown in Fig. 1a. Classically, the login identity is the user's first name, illustrated here, as "Smith" and an exemplary password is "Fido", their dog's name. For security purpose, each character of the password is replaced with a star on the display so that nobody can read it. Each time a user is prompted to enter his password, the password is always identical to the one previously entered by the user unless the user has modified their password during a previous session. An ill-intentioned person can easily find out this type of static password and freely enter a company's network system.

[0019] Optionally, to make the system more difficult to break, the network system is organized in such a way that regularly all the employees are prompted to enter a new password. Often, the system allows the users to combine a non-determined number of letters, either small or capital, and digits in their passwords. However, due to the multiplicity of the systems and the recurrence of the demand, employees often use the same password to which a number is just added. For example, the "Fido" password becomes after a change request "Fido1". During the time period lasting between two successive modifications of a password, the password remains unchanged. A competent person may rapidly find out the password of a user and access a company's network..

[0020] As mentioned, the fact that the password remains unchanged during a long period of time between two modifications renders the system insecure. It will be advantageous to provide a security system based upon a dynamic password, i.e. a password comprising at least one parameter that changes in an uncontrollable way.

[0021] A most probable parameter that is uncontrollably variable is a parameter related to time. It is therefore advantageous to introduce a parameter related to the time in a dynamic password generation process because the time can be used in many ways such as hour of the day, day of the week/month, age, etc. By introducing at least a time parameter into a dynamic password generating equation, a password is automatically and deterministically different nearly every time it is used. The password mostly comprises some static or passive parameters such as the name of the user and perhaps

also isolated letters that may complicate the determination of the password. An example of such a dynamic password generating equation is shown below:

[0022]  $\$hour + \text{"Smith2"} + \$mday + 23 + \text{"I"} + (\$hour + 16)/2$

[0023] Where the uncontrollably variable parameters are:

5                   , hour that represents the hour of the day, and mday that represents the day of the month.

[0024] Where the static parameters are:

                  Smith2 that represents the user's name and can be easily remembered by the user and I is an isolated letter.

10 [0025] The dollar sign indicates a variable parameter, and the quote sign is indicative of static parameters. Alternatively, the distinction between static and variable parameters is made another way or using other characters.

[0026] Assuming that a user wants to access the company's network at 8:22 am on May 25, and has the account Smith, she determines from the variable password  
15 equation her password at the present time. Here it is:

8Smith248I12

[0027] and enters it into the system which verifies it. Anyone trapping the password and storing it for later use will be sadly disappointed because the password will expire one hour later while Smith easily determines the correct password an hour later without  
20 needing to change the password on the system.

[0028] Of course, the predetermined equation shown here is just for illustrative purpose. In the present example, only two different variable parameters are in the equation, there is no limitation as to the number of these parameters or as to the number of static parameters. However, it is most probably difficult to introduce too many  
25 parameters in a single equation, either variable or passive, because the user has to remember them and their combination, and as such has to memorize at least the order in which the various parameters have to be entered. Advantageously, the parameters variable and passive are not difficult to memorize because they are certainly available and easily accessible by the user such as the hour of the day, the date or a name, a word  
30 of the day, etc.



[0029] Referring now to Fig. 2, a flow diagram of a method of validating a dynamic password is illustrated. The user needs to know the equation for generating the dynamic password. In the present example the equation is:

$$\text{\$hour} + \text{"Smith2"} + \text{\$mday} + 23 + \text{"I"} + (\text{\$hour} + 16)/2,$$

5           the user provides the hour of the day - "8" -, the characters "Smith2" followed by the value 48 being the day of the month plus 23, the letter "I" and 12 being  $(8+16)/2$ . The processor receives the string of characters for verifying the validity of the dynamic password. The processor generates a same password to verify that the user's password and then compares the characters within the string relative to the  
10           generated string according to the equation.

[0030] Eventually, a problem might rise when a password is entered at a time close to a change of the hour, for example. For example, assuming a variable parameter corresponds to the hour a user is entering a password, if the user's watch indicates 7:58 am, which is a time close to changing from 7 to 8, and the computer's watch has  
15           already turned over 8, the user might be rejected because the user password indicates a character 7 where the computer waits a 8. Even in these situations, it is easy for a user to either wait a few minutes or to realize that the system hour may be 7 or 8. Of course, synchronizing computers to the network password server clock will obviate this problem so long as users verify the time on their computers and not with their watches  
20           or desk clocks. Eventually, during a short period of time of a few minutes overlapping a change of hour as in the previous example, the network server accepts a password wherein the character indicative of the hour is incorrect within predetermined limits. In the previous example, the computer accepts password comprising the character 7 instead of 8 for indicating the hour. Similarly, if the user's watch indicates 8:02 am,  
25           and the computer's watch indicates 7:58 am, the computer accepts password comprising the character 8 instead of 7 for indicating the hour.

[0031] What may introduce a difficulty for a user are the numbers to memorize and eventually the operations to perform to complete the password. There are no prerequisites to incorporate operations in an equation for generating a dynamic  
30           password. Similarly, there is no prerequisite not to incorporate operations while

elaborating or programming the dynamic password generating equation for securing a network access.

[0032] In a further embodiment, the generation of a dynamic password relies again on a predetermined equation wherein an image is introduced as a parameter along with the variable and the static parameters. Referring to Fig. 3, a computer screen is displaying a plurality of images including various shapes, animals, trees, and different symbols. An image of a series as the one illustrated in Fig. 3 is part of a dynamic password generating equation. An example of such a dynamic password generating equation is shown below:

10 
$$\text{\$hour} + \text{"Smith2"} + \text{\$image}$$

Where the variable parameter is: hour that represents the time of the day.

Where the static parameter is: Smith2 - the user's name.

Where the image parameter is: image

[0033] Where the dollar sign indicates a variable parameter, the quote sign is indicative of a static parameter.

[0034] Assuming that the user wants to access her company's network at 8:22 am. An image is presented in the dialogue box asking for her password. For example, a tree may be displayed. In that instance, the user enters a password according to the above-predetermined dynamic password generating equation. The password will thus be in the form of:

8Smith2tree

[0035] Advantageously, an interpretation of the image is as valid as the image itself. For example, if the imaged tree is a pine, the password might reflect this particularity and incorporate the tree species. Moreover, English is not the exclusive language that can be used to describe a tree. Indeed, computers of large companies, especially international companies, are preferably programmed to accept passwords generated in any of a number of possible languages. Alternatively, only the user's mother tongue is accepted for a given password entry. Consequently, incorporating an image in the equation allows multiple other possibilities for the resulting password.

[0036] Back to the previous example and the possibilities allowed with a single image of a tree, here are 3 of the possible passwords:

8Smith2tree

8Smith2pine

5 8Smith2arbre

[0037] All the images are interpreted to a certain extent. For example, if an image of a bulb is selected, the possible words illustrating a bulb, notwithstanding a foreign language, might be lamp, idea, light, lightbulb, bulb, eureka, etc. Of course the flexibility in image identification is a parameter that is set during system  
10 implementation or alternatively as an option to be set by a system administrator.

[0038] Thus, generating a dynamic password incorporating an image in the equation along with the variable and the static parameters also makes the system less secure when variability of many parameters is supported. That said, since the image is not immediately discernible to an unauthorized individual and its location within the  
15 password is unknown, it is believed that overall security will increase when the system is used by unconcerned individuals – individuals who are not specially trained in computer security.

[0039] In the example shown here, only one variable, one static, and one image parameter form part of the predetermined equation for generating the password but of  
20 course, there is no limitation as to the number of these parameters. The limit that may be taken into consideration is the good will of the user as to his capacity to memorize parameters to enter when prompted to do so. Additionally, there is no prerequisite to incorporate operations in the equation for generating a dynamic password. Similarly, there is no prerequisite not to incorporate operations while elaborating or programming  
25 the dynamic password generating equation for securing a network access.

[0040] Even though a dynamic password offers enormous advantages over static passwords, it is beneficial to have the possibility to change the password from time to time to decrease drastically the possibility to compromise security of the system. A way to achieve such beneficial possibility is to assign a code to the different parameters  
30 that compose a dynamic password. A code might be of various forms as for example an

Arabic number, or a Roman numeral, or a letter, etc. The codes are assigned, for example, according to a predetermined setting or more probably are randomly assigned.

[0041] Referring to a previous example wherein the dynamic password generating equation was in the form of:

5                    Shour + "name2" + \$image

[0042] A first possibility is to determine as many codes as parameters in the equation. So in the present example, three codes are assigned:

	Possibility 1	Possibility 2	Possibility 3
	code 1 → hour	code 1 → name	code 1 → image
10	code 2 → name	code 2 → image	code 2 → hour
	code 3 → image	code 3 → hour	code 3 → name
	Possibility 4	Possibility 5	Possibility 6
	code 1 → hour	code 1 → name	code 1 → image
	code 2 → image	code 2 → hour	code 2 → name
15	code 3 → name	code 3 → image	code 3 → hour

[0043] An advantage in coupling codes to parameters is that the codes can be ordered arbitrarily by the server, allowing for a multiplicity of representations of a same password. Thus, intercepting the password equation is of limited value. Also, often codes are easier to enter than textual representations of parameters. Effectively, by changing the code assignment, the password though unchanged, appears differently to a Trojan Horse application and is therefore more difficult to decode. Also, it is unclear what each code entry refers to. Here, there exist 6 possibilities of reassigning the three codes to the three parameters, which leads to six different possible password entries resulting in the three identical parameters in the same sequence as in the Possibility 1.

25 [0044] To drastically increase the password's possibilities wherein the same dynamic and static parameters are initially required, the number of codes can exceed the number of parameters. For example, if 10 codes are available and 5 parameters are required for generating a dynamic password, the number of possibilities is increased according to the combination of 5 codes chosen from 10 to obtain an arrangement of the

parameters identical to the arrangement required in the equation. Consequently, the number of possibilities is increased by about 252. Of course, these numbers are cited for exemplary purpose only, the number of codes available is not limited to any of the mentioned numbers.

5 [0045] Static parameters as used in the specification denote parameters that do not change. These can include string values and defined answers to questions that do not change. For example, "iQw4" is a string. Another static parameter is a user's name, employee number, address, etc. Which are determined and unchanging parameters. Of course, the static parameters can also be identified within passwords by encoded value  
10 in order to make interception of the password during password changes more difficult.

[0046] When a system has access to a significant amount of data, it is also possible to relate the password to data known to the system. Some example variable parameters include: days to a new moon, days until a product release, days since year end, months since hiring, years since hiring, employee age in years, months since last vacation week,  
15 number of people on vacation within a person's group, amount on last paycheck, taxes deducted on last paycheck, amount in employee savings plan, and so forth. Also, posted data is useful such as today's lunch menu items, word of the day, and so forth.

[0047] In order to verify a password when provided, there are several possible methods. According to a preferred embodiment, the static portions of the password are  
20 hashed either separately or in a concatenated or other joined form. The hashed value is stored. When a password is received, it is separated into static and dynamic values. The dynamic values are regenerated to verify the dynamic values. The static values are hashed and the hash values are compared. As such, the resulting static portions are not stored on the server and cannot be detected by a snooping device. The dynamic  
25 parameters are stored in an encoded fashion that is typically other than human intelligible. For example, if 256 variable parameters are known, the variable parameters are stored as 8 bit values.

[0048] Alternatively, the dynamic values are verified without regenerating same. For example, if the variable parameter is day of month + 23, then the verification  
30 process merely subtracts 23 from the provided value and compares the result to the

present day of the month. Of course, other methods of password verification are possible.

[0049] Advantageously, the dual composition of these passwords, i.e. dynamic and static values renders the dynamic passwords usable with various existing system  
5 without requiring any other support. Typically, a password is used for activating encryption keys for encrypting data. Advantageously, the static values of a dynamic password are used as keys like typical passwords. However, the presence of dynamic values in combination with the static values in a dynamic password increases the security of the system. That said, even if static values are potentially accessible to an  
10 unauthorized individual, their location within the password is unknown. Therefore, accessibility to encryption data is possible thanks to the static values and moreover, the accessibility is protected by the dynamic values.

[0050] Numerous other embodiments might be envisioned without departing from the scope and the spirit of the present invention. For example, the description of the  
15 invention implicitly inferred that the dynamic password generating equation was identical for all the employees of a company. The difference between the dynamic passwords of two employees login in at the same time being the static parameters. However, each employee can have a specific dynamic password generating equation. The multiplicity of equations, i.e. as many equations as employees, might be  
20 advantageous if an employee leaves the company. In such a case, the equation is deleted and nobody else in the company is affected, otherwise, the whole system must adapt to the departure for keeping the system as secure as possible.

### Claims

What is claimed is:

- 5 1. A method of password verification comprising the steps of:  
providing a process for transforming at least a variable parameter into an  
ordered string of characters, wherein the process sometimes results in different ordered  
strings of characters for a same variable parameter;  
providing at least a variable parameter as a known password;  
10 determining from data available to an individual and from the known password  
a static string;  
providing the determined static string as a password for verification; and,  
verifying the static string to determine that it is an accurate transformation of the  
at least a variable parameter according to the provided process and when the  
15 determination is that the transformation is accurate, providing an indication that the  
password is verified.
2. A method according to claim 1, characterized in that the step of verifying the  
static string includes the steps of:  
20 performing the process for transforming at least a variable parameter on the  
known password to determine a second static string;  
comparing the provided static string with the second static string to determine a  
comparison result and,  
when the comparison result is indicative of a match, providing an indication that  
25 the password is verified.
3. A method according to claim 1, characterized in that the at least a variable  
parameter includes an uncontrollably variable parameter.
- 30 4. A method according to claim 2, characterized in that the at least a variable  
parameter includes at least a static parameter.

5. A method according to claim 1, characterized in that the process includes steps of determining from present time data, a current value for a variable parameter relating to time.

5 6. A method according to claim 1, characterized in that the process includes steps of providing data to a user for interpretation by the user and then comparing the user's interpretation to a predetermined known interpretation.

7. A method according to claim 6, characterized in that the provided data is an  
10 image and the interpretation is a string indicative of the image.

8. A method according to claim 1, characterized in that the known password is provided by a user.

15 9. A method according to claim 8, characterized in that the known password is entered as a string of characters and wherein at least a character is indicative of one of a variable parameter and a static parameter.

10. A method according to claim 9, characterized in that the string of characters is  
20 parsable to form the known password, the parsing distinguishing variable parameters from static parameters within the known password.

11. A method of changing dynamic passwords comprising the steps of:  
providing a string of characters, the string including indications of at least a  
25 parameter from a plurality of parameters, the at least a parameter being a variable parameter variable upon predetermined criteria;  
receiving the provided string of characters; and,  
storing data based on the known password, the data sufficient for verifying  
provided passwords to determine their accuracy.

30

12. A method of changing dynamic passwords according to claim 11, comprising the step of:



with a processor parsing the provided string of characters to distinguish static data from the at least a variable parameter.

13. A method of changing dynamic passwords according to claim 11, characterized  
5 in that the parameters are selected from a plurality of available parameters and characterized in that the plurality of available parameters are provided to a user for selecting therefrom.

14. A method of changing dynamic passwords according to claim 13, characterized  
10 in that the plurality of available parameters are each represented by an identifier and characterized in that the identifier for a given parameter in one instant is different from the identifier for a same parameter in another instant.

15. A method of changing dynamic passwords according to claim 11, characterized  
15 in that the step of storing data based on the known password comprises the steps of:  
extracting static data from the known password;  
hashing the extracted static data to determine at least a static hash value;  
storing the at least a static hash value; and,  
extracting dynamic data from the known password and storing indications of the  
20 dynamic data.

16. A method of verifying a dynamic password comprising the steps of:  
receiving a password comprising a string of characters wherein the characters  
are sequenced according to a predetermined sequence of variable parameters and static  
25 parameters;  
identifying static parameters within the string of characters;  
determining dynamic parameter values related to the dynamic parameters in  
accordance with the predetermined sequence ;  
comparing static parameters received within the string of characters with  
30 previously stored static parameters and the received dynamic parameter within the  
determined dynamic parameters to determine a first comparison result;  
wherein upon both the first comparison result being indicative of a match, the  
dynamic password is validated.

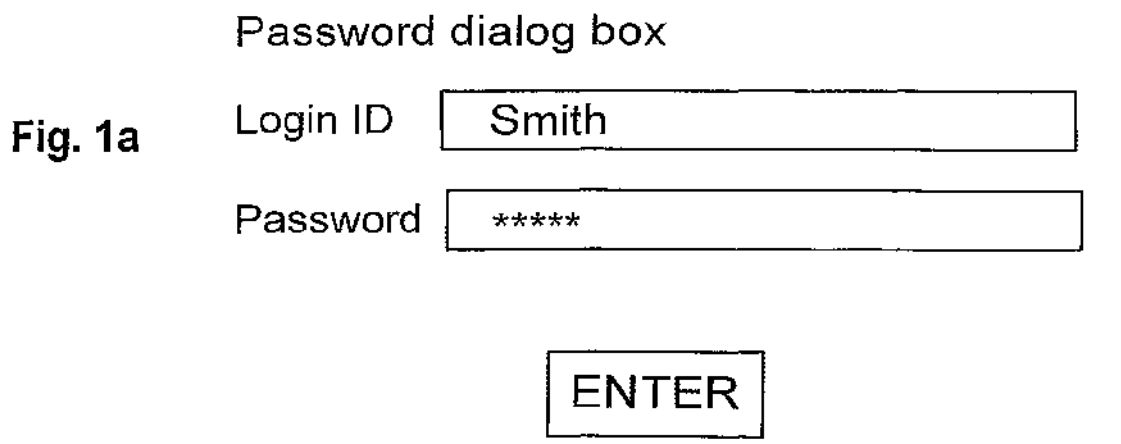
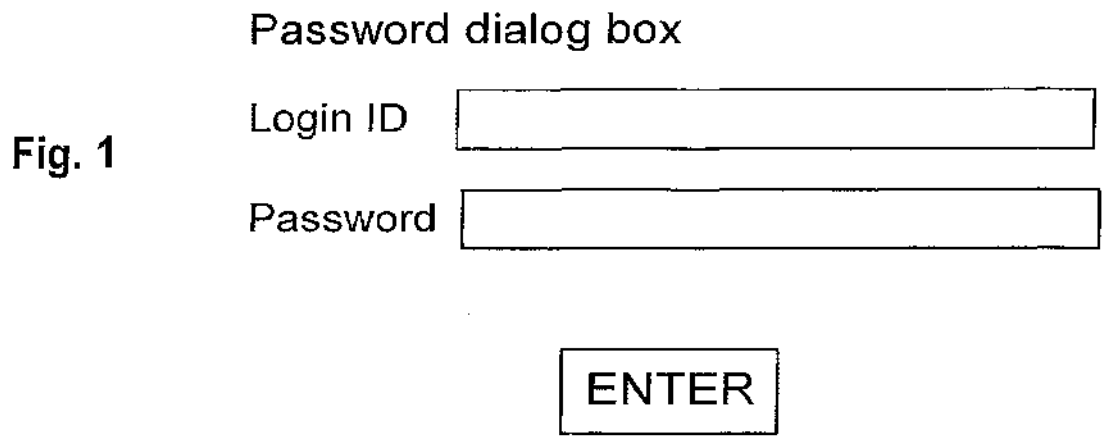
17. A method of generating a dynamic password comprising the steps of:  
providing a process for transforming at least a variable parameter into an  
ordered string of characters, wherein the process sometimes results in different ordered  
strings of characters for a same variable parameter; and,

5 providing at least a variable parameter as a password, the provided variable  
parameter provided by an individual via a data entry device.

18. A method of generating dynamic passwords according to claim 17,  
characterized in that the plurality of variable parameters comprises uncontrollably  
10 varying parameters.

19. A method of generating dynamic passwords according to claim 18,  
characterized in that the predetermined criteria for varying the variable parameters is  
characteristic of a time frame.

15



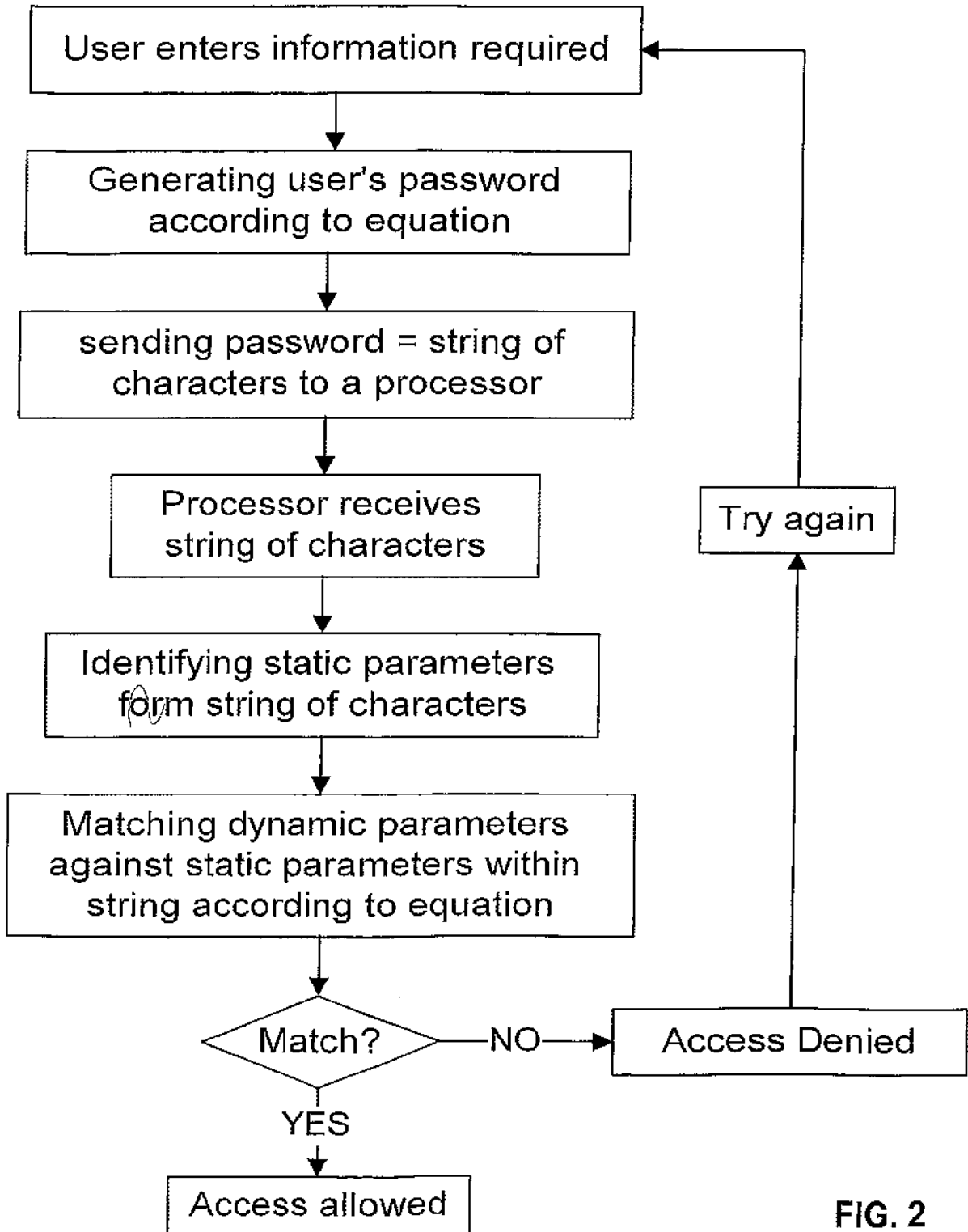


FIG. 2



FIG. 3

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
24 April 2003 (24.04.2003)

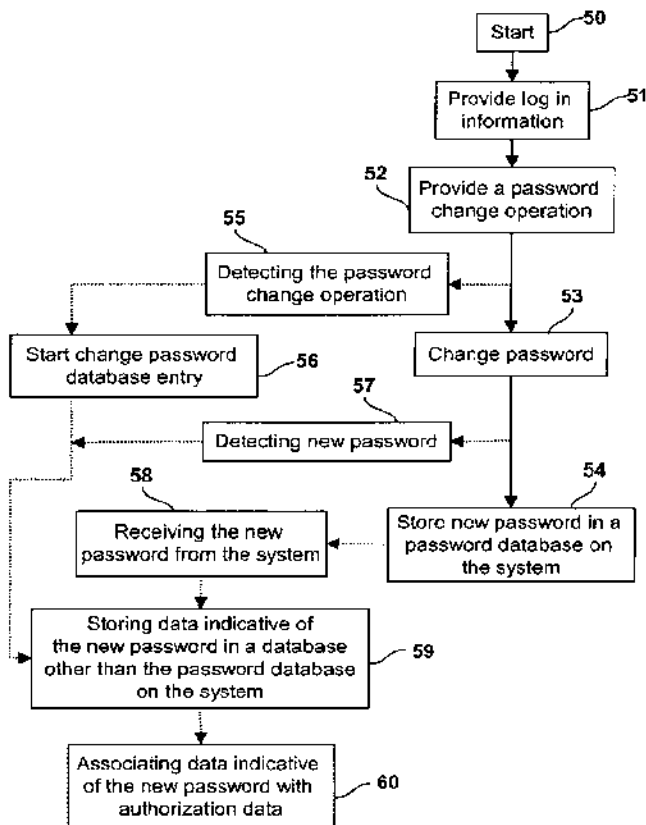
PCT

(10) International Publication Number  
**WO 03/034189 A2**

- (51) International Patent Classification<sup>7</sup>: G06F 1/00
- (21) International Application Number: PCT/JP02/11445
- (22) International Filing Date: 11 October 2002 (11.10.2002)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data:  
09/977,202 16 October 2001 (16.10.2001) US
- (71) Applicant: **ACTIVCARD IRELAND, LIMITED**  
[IE/IE]; 30 Herbert Street, 2 DUBLIN (IE).
- (72) Inventor: **CHARBONNEAU, Marc**, 23, Terrace Sauve,  
Casselman, OTTAWA, Ontario KOA 1M0 (CA).
- (74) Agent: **CABINET JP COLAS**; 37, avenue Franklin D.  
Roosevelt, F-75008 PARIS (FR).
- (81) Designated States (*national*): AT, 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, OM, PH, PL, PT, RO, RU, SD, SE, SG,  
SI, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VN,  
YU, ZA, ZM, ZW.
- (84) Designated States (*regional*): ARIPO patent (GH, GM,  
KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW),  
Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM),  
European patent (AT, BE, BG, CH, CY, CZ, DE, DK, EE,  
ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE, SK,  
TR), OAPI patent (BF, BJ, CI, CG, CI, CM, GA, GN, GQ,  
GW, ML, MR, NE, SN, TD, TG).

[Continued on next page]

(54) Title: METHOD FOR SUPPORTING SINGLE SIGN ON



(57) Abstract: A method of securely supporting password change is disclosed. The method comprises the steps of: detecting an occurrence of a password change operation (55) in execution on a system and receiving a new password by the system; detecting the new password when provided (57); storing data indicative (59) of the new password in a database other than the password database of the system for later retrieval, the data indicative of the new password for provision to the system.



WO 03/034189 A2



**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.*

## Method for Supporting Single Sign On

[001] The present invention relates to a method for changing password data, and more particularly, to a method for securely supporting password change for a central database of passwords independent of some processes with which the password is associated.

### Background of the invention

[002] Security is fast becoming an important issue. It is well known that with the proliferation of computers and computer networks into all aspects of business and daily life - financial, medical, education, government, and communications - the concern over secure file access is growing. Using passwords is a common method of providing security. Password protection and/or combination type locks are employed for computer network security, automatic teller machines, telephone banking, calling cards, telephone answering services, houses, and safes. These systems generally require the knowledge of an entry code that has been selected by a user or has been preset.

[003] In many large companies, the computer system is organized as a network to reduce the cost of purchasing and installing software on all the stations existing in the company. A main advantage of using a network is to facilitate data accessibility to each employee. However, it is necessary to limit access of a company's network to the company's employees. As such, prior to access the company's network, a password window prompted the company's employees to enter a login identity and an associated password. Usually, a user specifies passwords. Most users, being unsophisticated users of security systems, classically choose as the login identity their first name, and their dog's name as a password for example. Each time a user is prompted to enter his password, the password is always identical to the one previously entered by the user unless the user has modified his password during a previous session. As such, many password systems are easily accessed through a simple trial and error process.

[004] Optionally, to make the system more difficult to break, the network system is organized in such a way that regularly all the employees are prompted to change their



password, or are required to run a specific routine to change their password. Often, the system allows the users to combine a non-determined number of letters, either small or capital, and digits in their passwords. During the time period lasting between two successive modifications of a password, the password remains unchanged. A competent  
5 person may rapidly find out the password of a user and access a company's network.

[005] Optionally, a password is stored in a password database and user authorisation information such as biometric information, a digital key, a smart card, or a global password is required to retrieve the password. When the password is retrieved, it is provided to the password window. It is known to those skilled in the art that a  
10 biometric identification system accepts unique biometric information from a user and identifies the user by matching the information against information belonging to registered users of the system. Fingerprint sensing and matching is a reliable technique for personal identification and/or verification.

[006] The combination of a password and biometric information such as a  
15 fingerprint for example is beneficial because it increases the security and limits accessibility to a system. However, an association between a biometric information sample and a password also raises a problem when the password is changed. If an individual changes his password manually using, for example, a change password command of a password protected system, a next time he wants to access the system  
20 and provides his fingerprint, his old password is retrieved and provided to the password prompt. The old password is not current and therefore a message indicating that the password is incorrect is provided for the user. Thus, the user has to manually type in the new password. Eventually, the user can run a password change routine wherein the old password is provided along with the fingerprint, the new password  
25 typed in and the biometric sample assigned from then to the new password.

#### **Object of the Invention**

[007] To overcome such an inconvenience, it is an object of this invention to provide a method for automatically assigning a new password.

[008] It is another object of the present invention to provide a method of  
30 detecting a password change operation in a system and prompt for a new password.

[009] It is another object of the present invention to provide a method of detecting a password change command and authorizing a password change operation.

#### **Summary of the invention**

[0010] In accordance with the present invention, there is provided a method of securely supporting password change comprising the steps of: detecting at least one of the operations in execution on a system comprising: detecting a password change operation, and detecting a new password storage operation; performing an operation to change the password of a user to a new password in the system; storing the new password in a password database on the system; and storing data indicative of a new password for later retrieval of the new password by the system in a database independent of the change password operation and of the database where the new password is stored .

[0011] In accordance with another embodiment of the present invention, there is provided a method of securely supporting password change comprising the steps of: detecting a password change operation in execution on a system; displaying to a user a prompt for a new password, the prompt independent of the password change operation; receiving the new password; performing an operation to change the password of a user to a new password in the system; storing the new password in a password database on the system; and storing data indicative of a new password for later retrieval of the new password by the system in a database independent of the change password operation and of the database where the new password is stored..

[0012] In accordance with another embodiment of the present invention, there is provided a method of securely supporting password change comprising the steps of: detecting a password change operation in execution on a system; displaying to a user a prompt for authentication information, the prompt independent of the password change operation; receiving the authentication information; when the authentication information is indicative of a known user, providing a password associated with the user to the system; performing an operation to change the password of a user to a new password in the system; storing the new password in a password database on the system; and storing data indicative of a new password for later retrieval of the new

password by the system in a database independent of the change password operation and of the database where the new password is stored .

[0013] In accordance with another preferred embodiment of the present invention, there is provided a method of securely supporting password change comprising the steps of: detecting a password change operation in execution on a system; performing an operation to change the password of a user to a new password in the system; storing the new password in a password database on the system; and storing data indicative of a new password for later retrieval of the new password by the system in a database independent of the change password operation and of the database where the new password is stored; wherein the system has a known user authorized thereon, and wherein the step of performing an operation to change the password comprises the step of automatically generating a new password.

#### **Brief description of the drawings**

[0014] Exemplary embodiments of the invention will now be described in conjunction with the following drawings, in which:

[0015] Fig. 1 is a flow diagram of a prior art method of associating a password to a fingerprint upon a match of a fingerprint with an associated template;

[0016] Fig. 2 is an example of a prior art password window dialog display;

[0017] Fig. 2a is an example of a filled password window dialog box on a computer screen display;

[0018] Fig. 3 is a flow diagram of a prior art method of changing password;

[0019] Fig. 4 is a flow diagram of a prior art method of retrieving the password for provision to the system;

[0020] Fig. 5 is a flow diagram of a method of securely supporting password change in accordance with a preferred embodiment of the present invention;

[0021] Fig. 6 is a flow diagram of a method of securely supporting password change in accordance with another preferred embodiment of the present invention;

[0022] Fig. 7 is a flow diagram of a method of securely supporting password change in accordance with another preferred embodiment of the present invention; and,

[0023] Fig. 8 is a flow diagram of a method of securely supporting password change in accordance with another preferred embodiment of the present invention wherein a choice is given to the user.

#### **Detailed description of the invention**

[0024] In the prior art, many security systems involving imaging fingerprints to allow access for example to a building, to a specific area within a building, to a computer, are described. The security systems wherein biometric information is used for identifying and authorizing access to an individual mostly rely on a prior art method as shown in Fig.1. Following a starting step 10, after a biometric information sample, in a form of a fingerprint for example, has been provided to a system at step 11, in order to generate a fingerprint, a fingertip is imaged to generate an image thereof, which is called a fingerprint or a fingerprint image. The fingerprint is then characterized at step 12. During the process of identification, the characterized fingerprint is compared to stored templates associated with fingerprints of the person at step 13 – for a one-to-one identification system - or of any person registered for access the system – in a one-to-many identification system. Upon a positive result of the comparison, when there is a match between the provided fingerprint and a stored template associated with a fingerprint at step 14, the system provides at step 15 a password associated with the stored template to, for example, a legacy password based system and the user is identified and authorized at step 16.

[0025] Referring to Fig. 2, an example of a screen display prompting an employee to enter a login identity in 21 and an associated password in 22 to allow the employee to access the network. An example of the display of Figure 1 filled in is shown in Fig. 2a. Classically, the login identity is the user's name, illustrated here, as "Smith" in 23. For security purpose, each character of the password is replaced with a star on the display so that nobody can read it as shown in 24. Each time a user is prompted to enter his password, the password is always identical to the one previously entered by the user unless the user has changed his password during a previous session.

[0026] Optionally, to make the system more difficult to break, the network system is organized in such a way that, regularly, all the employees are prompted to enter a new password in order to change the passwords at regular intervals. Often, the system allows the users to combine a non-predetermined number of letters, either small or capital, and digits in their passwords. Referring to Fig. 3, a prior art method of changing passwords is shown. After a starting step 30, in order to access a system at step 32, the password change window prompts a user to provide an identity and the old password associated with the provided identity at step 31. Once authorized, the user is able to provide the system with a new password at step 33. Typically, the user is prompted to type in a new password two times as shown at step 34. The new password is stored in a password database of an application or operating system related to the password change operation on the system and now replaces the old password at step 35 before an ending session at 36.

[0027] Referring now to Fig. 4, a flow diagram of a method of retrieving the password for provision to the system is shown. For accessing a system after a starting step 40, a user provides authorization data at step 41, in the form of biometric information sample or information stored on a smart card. The authorization data is verified and is used to retrieve data indicative of the user password at step 42. Upon provision of the authorization data, the password is retrieved from a database other than the password database of the system or application at step 43 and provided to the system or application so that the user can gain access thereto.

[0028] The authorization data permits identifying a user based on, for example, biometric information provided therefrom. This provides an indication that the correct person was actually present when the request for changing a password was provided. A major advantage of using biometric information for retrieving a password is that the password does not have to be memorized. Typically, the user provides biometric information from a biometric source. The biometric information is characterized, processed and compared against templates stored in the system. Upon a match of the features extracted from the templates and the characterized biometric information corresponding to the biometric source provided by the user, an authorization signal is either provided or denied.

[0029] Referring now to Fig. 5, a method for securely supporting password change in accordance with a preferred embodiment is shown. To facilitate the comprehension of the figure, lines are plain for showing a classic password change routine flow, whereas dashed lines show changes in process flow for securely supporting password change. Each individual also has access from its workstation to a password change command. It is understandable that when a user has any doubt concerning the confidentiality of his password, he can change it independently of a network administrator. The user accesses the system at step 50 and provides a command for a password change operation to be performed on the system at step 52. Usually, the user is prompted to type in a new password twice as disclosed with reference to Fig. 3 at step 53, and then the new password is stored in a password database on the system at step 54. Inconveniently, the password is changed independently of the authorization data or log in information when the system supports user authorization and password retrieval as disclosed with reference to Fig. 4. Therefore, the next time the user tries to access the system, his password information will not match with the new password – it has not been updated, and access will be denied.

[0030] According to the present invention, when a change password operation in execution on the system occurs, it is detected at step 55. That said, any password change command options in the form for example of the word “password” or the abbreviation “pwd” typed in are recognized. Of course, though it is preferred that all possible password change operations are detected, the present invention is advantageous if even a single change password operation is detected. The new password is changed at step 53 and the new password is stored in the password database on the system at step 54. Approximately simultaneously, the new password is detected by another process at step 57 that uses the detected data to change the password in another database at step 59. For example, the data indicative of the new password is automatically associated with the authorization data within a system at step 60 such as that of Fig. 4. Therefore, for future accesses to the system, the user just provides his authorization data in a form of a fingerprint for example, the system retrieves the data indicative of the new password associated with the authorization data and the user is authorized to access the system.

[0031] Alternatively, the storage of the new password in a password database on the system is detected and data indicative of the new password are also detected for storing in a database other than the password database on the system as shown at step 58.

5 [0032] Interestingly, the user is not aware of the detection procedure and of the automatic assignment of the authorization data to the data indicative of the new password. Therefore, the user types in a new password twice for storing the new password in a password database on the system, data indicative of the new password is saved in a database other than the password database on the system at step 59 and the  
10 password is changed on the system, and the user does not have to retype this new password for further access. However, because of the transparency of such a system, the user does not know whether his new password has effectively been changed or not.

[0033] Referring now to Fig. 6, a flow diagram of a method of securely supporting password change in accordance with another preferred embodiment of the present  
15 invention is shown. When a password change operation is provided at step 61, the password change operation is detected at step 61 and a secure password change process prompts the user for a new password at step 63 to allow the change password operation to proceed at step 64. The new password is provided to the process at step  
20 65 to allow changing of the password, which is stored in an independent database at step 66. The data indicative of the new password is automatically associated with the authorization data in replacement of the data indicative of the old password. From the independent database, the new password is provided to a password database on the system at step 67 to change the password there. The prompt for a new password by the secure password change process instead of by the process associated with the  
25 system or application notifies the user that the password change operation has been detected and that the new password is accurately stored.

[0034] Advantageously, the above process is implemented with no apparent change to the users of the system. In other words, a user is completely unaffected by the method of Fig. 6, since it is transparent to the user and does not affect any existing  
30 change password processes.

[0035] Referring now to Fig. 7, a flow diagram of a method of securely supporting password change in accordance with another preferred embodiment of the present invention is shown. When a password change operation is provided at step 70, the password change operation is detected at step 71 and a secure user authorization process prompts the user for an authorization data at step 72. Once authorized at step 5 73, the system allows the change password operation to proceed at step 74. The new password is provided to allow changing of the password, which is stored in an independent database at step 75. The data indicative of the new password is automatically associated with the user identity in replacement of the data indicative of the old password. From the independent database, the new password is provided to a 10 password database on the system at step 76 to change the password there. The prompt for user authorization data by the secure authorization process instead of by the process associated with the system or application notifies the user that the password change operation has been detected and that the new password is accurately stored.

15 [0036] The above process is highly advantageous. It provides a single password change process and as such a single ergonomic interface for changing passwords. Therefore, design and implementation of the secure change password process replaces all legacy change password processes allowing for better information for the users and a more modern and ergonomic process.

20 [0037] Further advantageously, the above process allows for changing of passwords of several systems/files/applications simultaneously. Thus, a single change password operation is used where before several or several hundred processes would have been required. This is most applicable when changing a password used to protect a single file such as a Microsoft ® Word® file or the like.

25 [0038] Of course, it is evident to those of skill in the art that a password entered in accordance with the above described process is optionally long and complex since there is no need to remember the password. Because of the automatic password retrieval, a user never needs to know their password so an arbitrary string of characters such as “efkjhgshgdxfbkj#\$\$JHYT\$kjsfd\*(&REW^kvhgfd)(\*^\*&^%C^Tvc 30 hbjhf86%(%(ffgf nm.b.nm.,mn.vb2609” is usable as a password allowing for greatly increased security.



[0039] Another advantage to the present method is that it allows tracking of old passwords to provide for access to older system restorations or old files that were saved using earlier passwords.

5 [0040] Of course, the process also supports different passwords for different systems, files and applications without substantial user inconvenience. This is achieved by storing each password in association with data indicative of the user identity or authorization and the system, file, or application with which the password is to be used. Of course, more complex associations are also possible when desired.

10 [0041] Referring now to Fig. 8, a flow diagram of a method of securely supporting password change for use with the method of Figure 7 wherein a choice is given to the user is shown. During the password change operation of step 80 and after user authorization at step 82 due to the detection of the password change operation at step 81, the user is given the opportunity to either enter a password or to have the process automatically generate a new password at step 83. Therefore, in the case of a  
15 computer-generated password, the user does not have to invent and remember the new password because it is automatically assigned to his authorization data and automatically retrieved for access to the system. Consequently, choosing a computer-generated password means that the new password is never typed in which decreases the possibilities of a Trojan Horse application from detecting same.

20 [0042] Advantageously, when a password is automatically generated, it is unknown to the user. This makes the password impossible to ascertain except by breaching security of password database. For example, when automatic password generation is used, an encryption key may form each password allowing for security relating to access and for encryption of file data to prevent mining of file data.

25 [0043] Numerous other embodiments may be envisaged without departing from the spirit and scope of the invention.

**Claims**

What is claimed is:

1. A method of securely supporting password change comprising the steps of:  
5 detecting at least one of the operations in execution on a system comprising:
  - (i) detecting a password change operation (55; 62; 71; 81),
  - (ii) and detecting a new password storage operation (57);performing an operation to change the password of a user to a new password in  
the system (53, 64, 74);  
10 storing the new password in a password database on the system (54; 67; 76);  
and,  
storing data indicative (59, 66; 75) of a new password for later retrieval of the  
new password by the system in a database independent of the change password  
operation and of the database where the new password is stored.  
15
2. A method of securely supporting password change according to claim 1  
wherein the step of detecting a password change operation (55; 62; 71; 81) in  
execution on a system comprises the step of detecting a new password prompt.
- 20 3. A method of securely supporting password change according to claim 1  
comprising the steps of:
  - prompting a user to provide authorization data (72); and,
  - associating the authorization data with the password.
- 25 4. A method of securely supporting password change according to claim 1,  
wherein the step of detecting the new password comprises the step of detecting the  
new password at least two separate times.
5. A method of securely supporting password change according to claim 1  
30 wherein the operation detected is a password change operation and further comprising  
the steps of:
  - displaying to a user a prompt for a new password (63), the prompt independent  
of the password change operation;

receiving the new password (65);

6. A method of securely supporting password change according to claim 5 wherein the step of detecting the change password operation in execution on a system comprises the step of detecting password change command options.

7. A method of securely supporting password change according to claim 1 wherein the operation detected is a password change operation and further comprising the steps of:

10 displaying to a user a prompt for authentication information (72), the prompt independent of the password change operation;

receiving the authentication information (73);

when the authentication information is indicative of a known user, performing said operation to change the password (74) of the known user to a new password in the system; and;

8. A method of securely supporting password change according to claim 7 wherein the prompt for authentication information is a prompt for biometric information.

20

9. A method of securely supporting password change according to claim 8 comprising the step of:

providing biometric information;

processing the provided biometric information to provide biometric data;

25 comparing the biometric data with a stored template; and

in dependence upon a comparison result retrieving a user password from a database.

10. A method of securely supporting password change according to claim 7 wherein the prompt for authentication information is a prompt for information stored on a smart card.

30

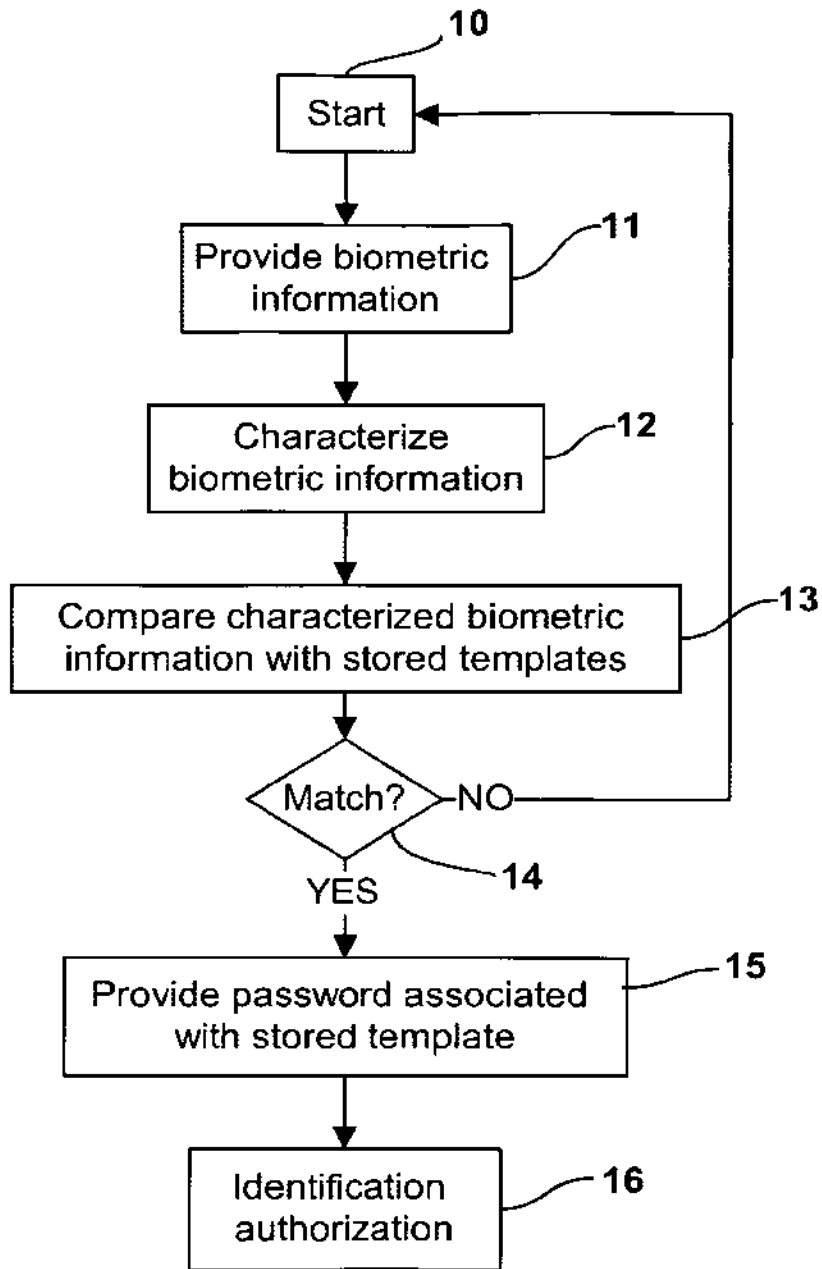
11. A method of securely supporting password change according to claim 7 wherein the step of performing an operation to change the password comprises the step of providing the new password to the system.
- 5 12. A method of securely supporting password change according to claim 7 wherein the step of performing an operation to change the password comprises the step of prompting the user to select between provision of the new password and automatic generation of the new password (83).
- 10 13. A method of securely supporting password change according to any of claims 7 and 12, characterized in that the step of performing an operation to change the password comprises the step of automatically generating the new password.
14. A method of securely supporting password change according to claim 13  
15 wherein data secured with the new password is encrypted using an encryption key.
15. A method of securely supporting password change according to claim 7 comprising the step of performing another operation to change another password of the known user to the new password.
- 20 16. A method of securely supporting password change according to claim 7 comprising the step of determining all passwords identical to the password being changed and automatically performing at least another operation to change each identical password of the known user to the new password.
- 25 17. A method of securely supporting password change according to claim 1 wherein the operation detected is a password change operation;  
wherein the system has a known user authorized thereon; and,  
wherein the step of performing an operation to change the password comprises  
30 the step of automatically generating a new password .

18. A method of securely supporting password change according to any of claims 13 and 17, characterized in that the automatically generated new password is unknown to the user.

5 19. A method of securely supporting password change according to any of claims 13 and 18, characterized in that the automatically generated new password is an encryption key.

10 20. A method of securely supporting password change according to any of claims 13 and 19, characterized in that the data secured with the new password is encrypted using an encryption key.

1/8



**Fig. 1**  
**(PRIOR ART)**

Password window

Log in ID  21

Password  22

**Fig. 2**  
(PRIOR ART)

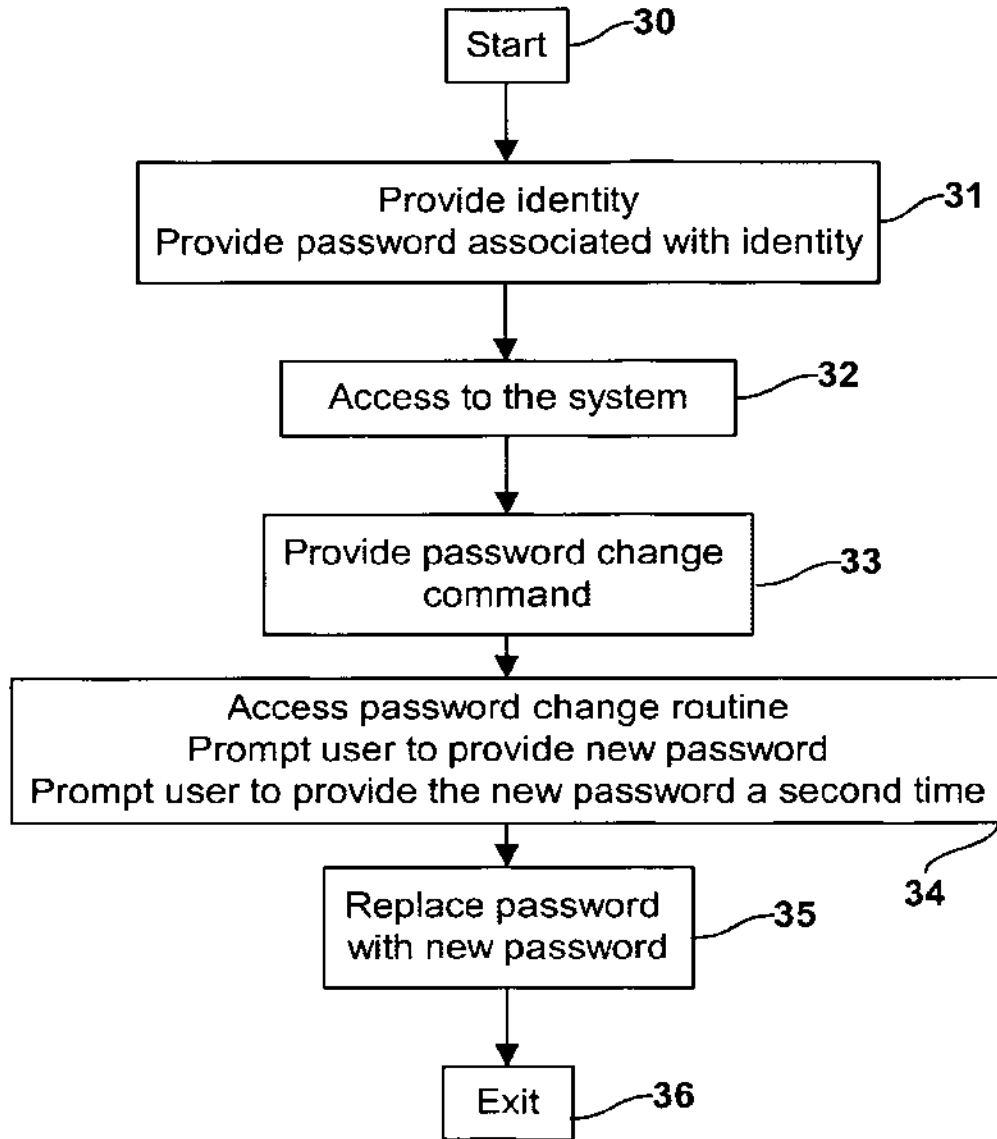
Password window

Log in ID  23

Password  24

**Fig. 2a**  
(PRIOR ART)

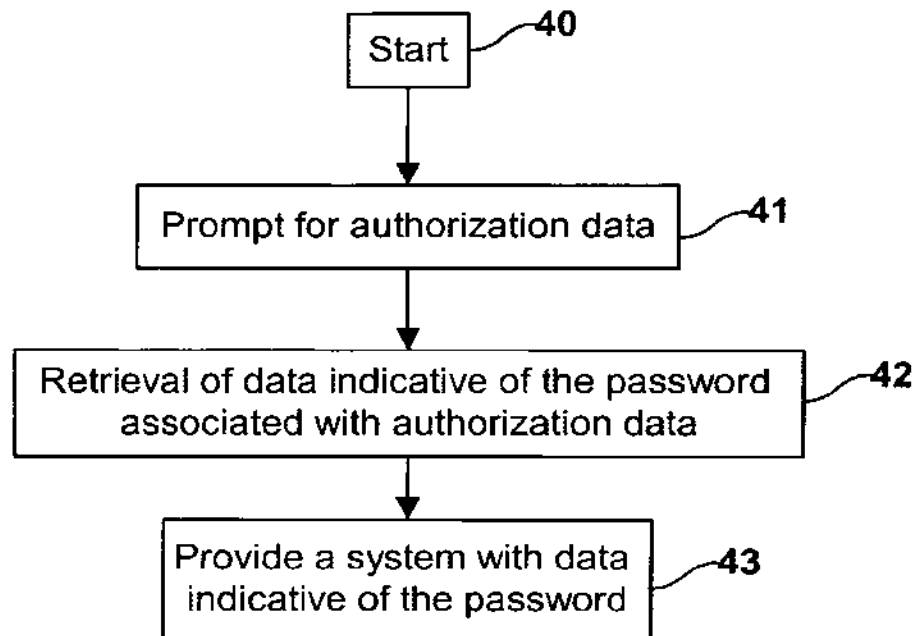
3/8



**Fig. 3**  
**(PRIOR ART)**



4/8



**Fig. 4**  
**(PRIOR ART)**

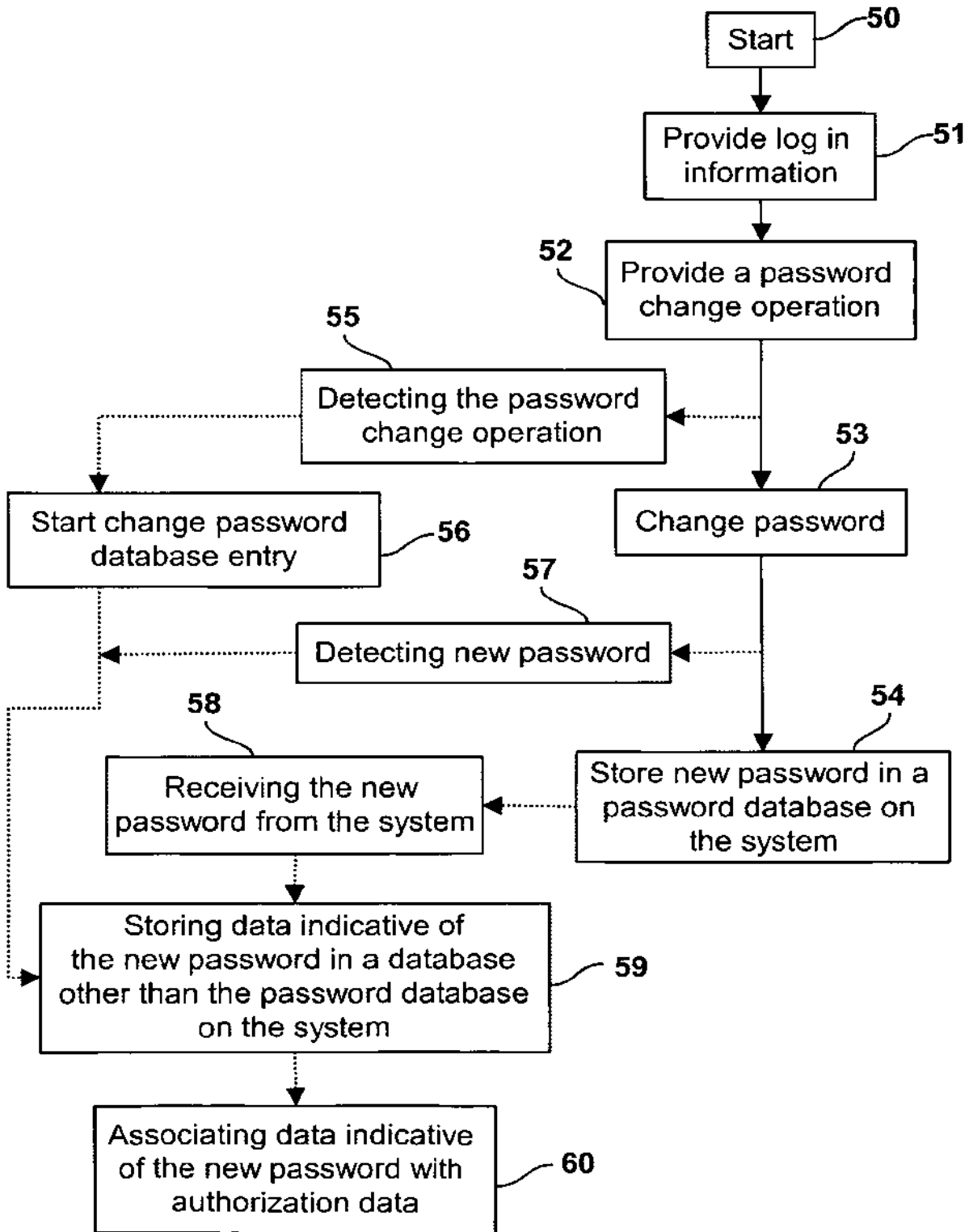


Fig. 5

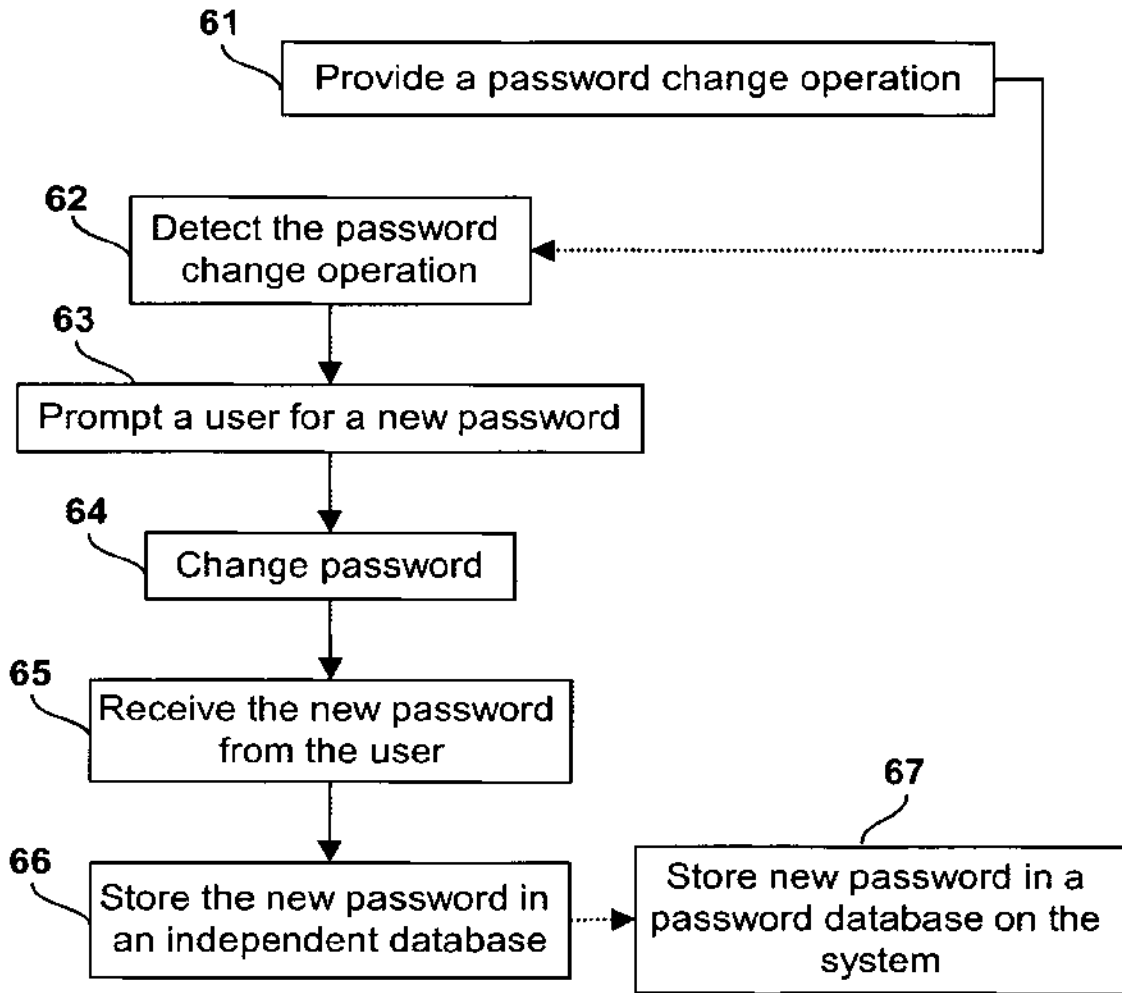


Fig. 6

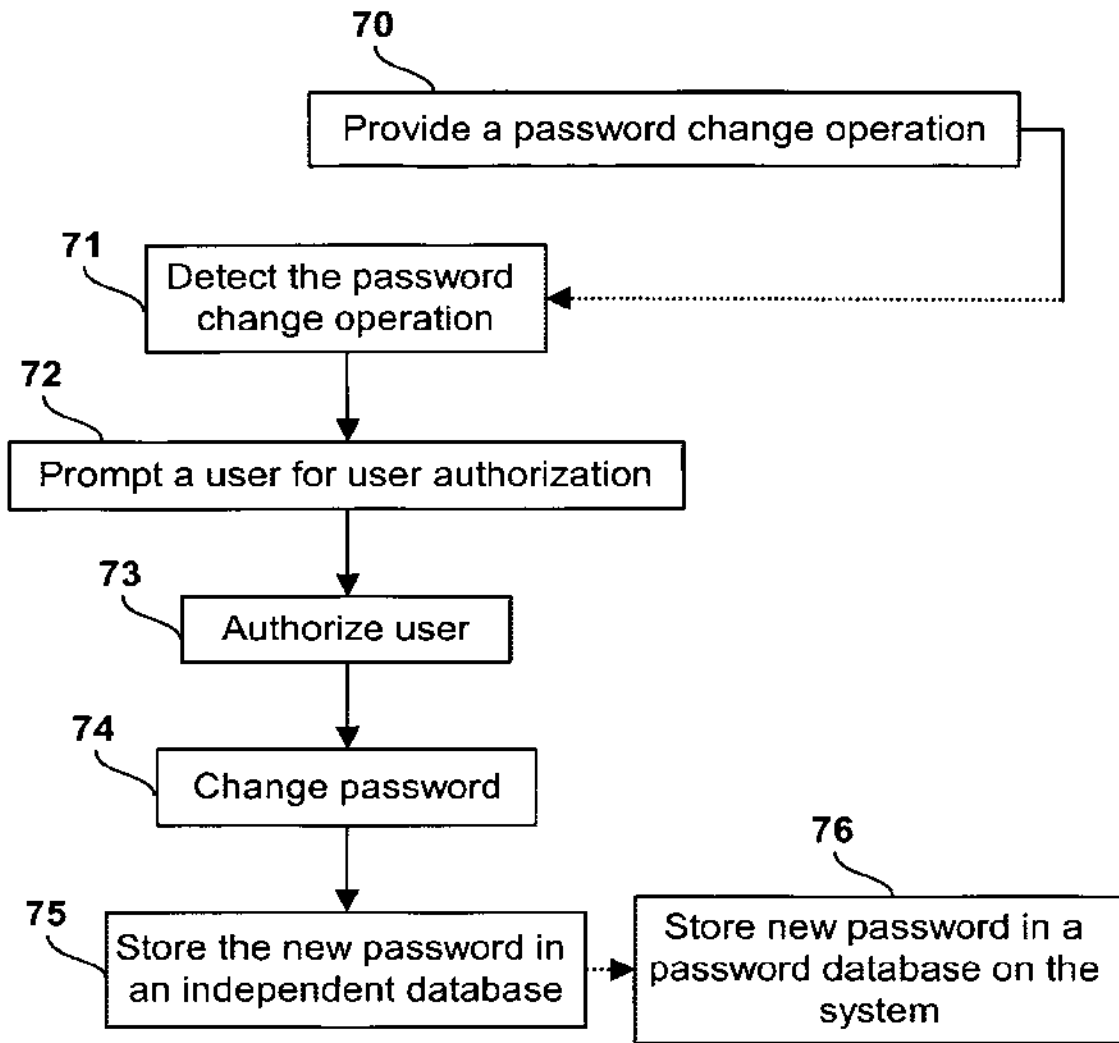


Fig. 7

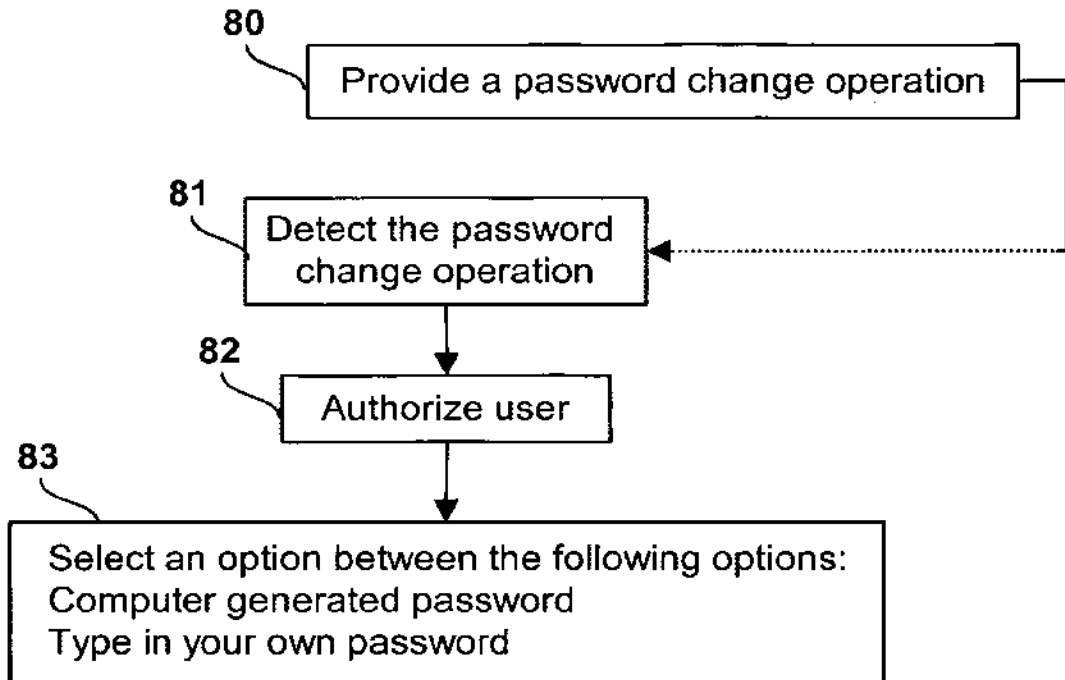


Fig. 8

(12) DEMANDE INTERNATIONALE PUBLIÉE EN VERTU DU TRAITÉ DE COOPÉRATION  
EN MATIÈRE DE BREVETS (PCT)

(19) Organisation Mondiale de la Propriété  
Intellectuelle  
Bureau international



(43) Date de la publication internationale  
31 décembre 2003 (31.12.2003)

PCT

(10) Numéro de publication internationale  
WO 2004/002058 A2

(51) Classification internationale des brevets<sup>7</sup> : **H04L 9/30**

(21) Numéro de la demande internationale :  
PCT/TR2003/001871

(22) Date de dépôt international : 18 juin 2003 (18.06.2003)

(25) Langue de dépôt : français

(26) Langue de publication : français

(30) Données relatives à la priorité :  
02/07688 19 juin 2002 (19.06.2002) FR

(71) Déposant (pour tous les États désignés sauf US) : **GEM-PLUS** [FR/TR]; Parc d'Activités de Gémenos, Avenue du Pic-de-Bertagne, F-13420 Gémenos (FR).

(72) Inventeurs; et

(75) Inventeurs/Déposants (pour US seulement) : **FEYT, Nathalie** [FR/TR]; 8, chemin de Raphèle, 7 lotissement l'Oliveraie, F-13780 Cuges les Pins (FR). **JOYE, Marc** [FR/TR]; 19, rue Voltaire, F-83640 Saint Zacharie (FR).

(74) Mandataire : **AIVAZIAN, Denis**; Gemplus la Vigie, Service brevets, BP 100, F-13705 La Ciotat Cedex (FR).

(81) États désignés (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, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) États désignés (régional) : brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet

européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CI, CG, CO, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Déclarations en vertu de la règle 4.17 :

— relative à l'identité de l'inventeur (règle 4.17.i) pour les désignations suivantes 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, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CI, CG, CO, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

— relative au droit du déposant de demander et d'obtenir un brevet (règle 4.17.ii) pour les désignations suivantes 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, NI, NO, NZ, OM, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, brevet ARIPO (GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), brevet eurasien (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), brevet européen (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), brevet OAPI (BF, BJ, CI, CG, CO, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)

[Suite sur la page suivante]

(54) Title: METHOD OF GENERATING ELECTRONIC KEYS FOR A PUBLIC-KEY CRYPTOGRAPHY METHOD AND A SECURE PORTABLE OBJECT USING SAID METHOD

(54) Titre : PROCÉDE DE GENERATION DE CLES ELECTRONIQUES POUR PROCÉDE DE CRYPTOGRAPHIE A CLE PUBLIQUE ET OBJET PORTATIF SECURISE METTANT EN OEUVRE LE PROCÉDE

(57) Abstract: The invention relates to a method of generating electronic keys (d) for a public-key cryptography method using an electronic device. The inventive method comprises two separate calculation steps, namely: step A consisting in (i) calculating pairs of prime numbers (p, q), said calculation being independent of knowledge of the pair (e, l) in which e is the public exponent and l is the length of the key of the cryptography method, and (ii) storing the pairs thus obtained; and step B which is very quick and can be executed in real time by the device, consisting in calculating a key d from the results of step A and knowledge of the pair (e, l).

(57) Abrégé : L'invention concerne un procédé de génération de clés électroniques d pour procédé de cryptographie à clé publique au moyen d'un dispositif électronique. Selon l'invention, le procédé comprend deux étapes de calcul dissociées. Une étape A consiste à - calculer des couples de nombres premiers (p, q), ce calcul est indépendant de la connaissance du couple (e, l) e l'exposant public et l la longueur de la clé du procédé de cryptographie et à - stocker les couples ainsi obtenus. Une étape B très rapide qui peut être exécutée en temps réel par le dispositif, consiste à calculer une clé d à partir des résultats de l'étape A et de la connaissance du couple (e, l).



WO 2004/002058 A2



- *relative au droit du déposant de revendiquer la priorité de la demande antérieure (règle 4.17.iii) pour toutes les désignations*
- *relative à la qualité d'inventeur (règle 4.17.iv) pour US seulement*

*En ce qui concerne les codes à deux lettres et autres abréviations, se référer aux "Notes explicatives relatives aux codes et abréviations" figurant au début de chaque numéro ordinaire de la Gazette du PCT.*

**Publiée :**

- *sans rapport de recherche internationale, sera republiée dès réception de ce rapport*

PROCEDE DE GENERATION DE CLES ELECTRONIQUES POUR  
PROCEDE DE CRYPTOGRAPHIE A CLE PUBLIQUE ET OBJET  
PORTATIF SECURISE METTANT EN ŒUVRE LE PROCEDE

L'invention concerne un procédé de génération de  
5 clés électroniques pour procédé de cryptographie à clé  
publique. Elle concerne également un objet portatif  
sécurisé mettant en œuvre le procédé.

L'invention concerne plus particulièrement la  
génération de clés d'un système cryptographique de type  
10 RSA et leur stockage sur un objet sécurisé en vue de  
leur utilisation dans une application nécessitant de la  
sécurité.

L'invention s'applique tout particulièrement à des  
objets sécurisés ne possédant pas d'importante  
15 ressource mémoire telle que de la mémoire  
électriquement programmable, ni de ressources de calcul  
puissantes comme c'est le cas pour les cartes à puce.

Une application de l'invention est le commerce  
électronique par l'intermédiaire d'un téléphone  
20 portable. Dans ce contexte les clés peuvent se trouver  
sur la carte SIM du téléphone.

Il est en effet prévu que certains programmes  
d'applications utilisent de telles clés pour mettre en  
œuvre un transfert de données confidentielles, dans un  
25 contexte de commerce électronique par exemple. Par la  
suite, on considèrera que ces applications sont  
fournies par une entité fournisseur de service.

En outre, il est connu que pour garantir  
l'intégrité de la clé, on lui associe généralement un  
30 certificat fourni par une entité de confiance.



Parmi les procédés de cryptographie à clé publique, on s'intéresse dans ce qui suit au protocole de cryptographie RSA (Rivest Shamir et Adleman). Ce protocole met en œuvre une étape de génération de  
5 nombres premiers de grande taille, coûteuse en temps de calcul et en place mémoire.

On rappelle que ce protocole de cryptographie RSA permet le chiffrement d'informations et/ou l'authentification entre deux entités et/ou la  
10 signature électronique de messages.

Le protocole de cryptographie RSA est le plus utilisé car il possède des propriétés qui lui permettent d'être employé aussi bien en chiffrement qu'en génération de signature.

Pour ce faire, le système de cryptographie RSA comprend un algorithme « public » réalisant la fonction de chiffrement ou de vérification de signature et un algorithme « privé » réalisant la fonction de déchiffrement ou de génération de signature.

Sa sécurité repose sur la difficulté de factorisation d'un nombre entier public  $N$  de grande taille qui est le produit de deux nombres premiers secrets  $p$  et  $q$  de grande taille, le couple  $(p, q)$  entrant dans le calcul de la clé secrète  $d$  utilisée par  
25 la fonction de déchiffrement ou par la fonction de calcul d'une signature.

Afin de mieux comprendre le problème qui va être exposé dans la suite, on va rappeler dans ce qui suit les paramètres entrant dans un schéma de cryptographie RSA :.  
30

1) L'exposant public  $e$  :

Il est propre à une application et est fourni par cette application. De ce fait, il est commun à tous les utilisateurs de cette même application.

2) Les paramètres  $p$  et  $q$ :

5 Ils sont générés à l'issu d'un calcul coûteux en temps. Ils ont en général la même longueur (même taille). Cette longueur est classiquement de 512 bits. Pour augmenter la sécurité, cette longueur peut aller de 512 bits à 2048, 2048 bits étant envisagés pour le  
10 futur.

3)  $N$  est le module public et est calculé à partir de la relation suivante :

$$N = p \cdot q$$

La clé de l'algorithme est dite de longueur  $\ell$ ,  
15 lorsque le module public  $N$  est de longueur  $\ell$ . Cette longueur est fixée par l'application (ou fournisseur de service).

4) les paramètres  $e$  et  $N$  forment la clé publique.

5) la clé privée  $d$  est calculée à partir de la  
20 relation suivante :

$$d = 1/e[\text{mod}(p-1)(q-1)] ; (1/e = e^{-1})$$

soit encore  $ed \equiv 1 \pmod{\text{ppcm}(p-1, q-1)}$  ;  $\text{ppcm}$   
signifie le plus petit commun multiple,

les paramètres secrets sont formés par le triplet  
25  $(d, p, q)$ .

6) la forme « normale » de la clé privée est:

$$(d, N).$$

6) la forme CRT (Chinese Remainder Theorem) de la  
clé privée est:

30 dans ce cas la clé privée comporte 5 paramètres :

$$p, q$$

$$d_p \text{ avec } d_p = d \text{ mod}(p-1)$$

$$d_q \text{ avec } d_q = d \text{ mod}(q-1)$$

$$I_q \text{ avec } I_q = q^{-1} \text{ mod} p.$$

Le principe de la génération d'une clé selon le schéma RSA consiste donc comme on peut le voir, à générer une clé privée  $d$  à partir d'un exposant public  $e$  (ou clé publique) fixé par l'application, les paramètres  $p$ ,  $q$  étant générés de sorte que  $p \cdot q = N$ , la longueur  $\ell$  de  $N$  étant fixée.

Lorsque plusieurs applications sont prévues, chaque fournisseur de service fournit son exposant public  $e$  et la longueur du module public  $N$ , de manière à ce que puisse être générée la clé privée  $d$  correspondante.

Ainsi, la mise en œuvre d'un calcul de clé RSA nécessite la connaissance de l'exposant public  $e$  et celle de la longueur  $\ell$  de la clé de l'algorithme c'est à dire la longueur du modulo  $N$ . Avec les données d'entrée  $e$  et  $\ell$ , il reste à générer le couple de nombre premier  $p$  et  $q$  de manière à ce que ces derniers répondent aux conditions suivantes :

- (i)  $p-1$  et  $q-1$  premiers avec  $e$  et,
- (ii)  $N = p \cdot q$  un nombre entier de longueur  $\ell$ .

Ces contraintes sont coûteuses en temps de calcul.

On rappelle à ce propos que la génération et le stockage des clés pour des objets portables tels que les cartes à puce s'effectuent à ce jour des deux manières suivantes :

Selon une première manière, le calcul d'une clé RSA est effectué sur un serveur pour profiter d'une puissance de calcul importante. On requiert alors pour plus de sécurité, un certificat que l'on télécharge avec la clé au sein de l'objet sécurisé lors de sa phase de personnalisation.

Cette solution présente deux inconvénients. :

- d'une part malgré le cadre relativement sécurisé de la personnalisation, il peut y avoir vol ou duplication de la clé du fait de son transfert du serveur vers l'objet sécurisé, et

5 - d'autre part, chaque clé est chargée dans l'objet dans une phase initiale de personnalisation, ce qui nécessite de prévoir un maximum de clés dans chaque objet pour pouvoir anticiper les futurs besoins.

10 Dans la pratique, on stocke dans l'objet portable des ensembles de clés et de certificats correspondant à chaque application susceptible d'être utilisée, sans savoir si ces clés seront réellement utiles ultérieurement. Un emplacement mémoire important est utilisé inutilement. Par exemple 0,3 Koctets sont

15 nécessaires pour une clé de RSA de module de 1024bits, alors que les cartes actuelles ont au plus 32Koctets de mémoire programmable. En outre, un nombre important de certificats est acheté à l'entité de confiance ce qui est coûteux.

20 L'inconvénient ultime mais tout aussi important est qu'il n'est pas possible d'ajouter de nouvelles clés au fur et à mesure que de nouvelles applications pourraient être envisagées.

25 Selon une deuxième solution, le calcul peut être effectué au sein de l'objet sécurisé. Cela résout le premier inconvénient de la solution précédente mais crée une lourdeur de traitement au niveau de l'objet sécurisé qui possède une faible capacité de calcul.

30 En effet, lorsque la génération d'une clé RSA est réalisée par un objet portatif tel qu'une carte à puce, si la longueur imposée de clé RSA est de 2048 bits, le calcul prend alors 30 secondes avec un algorithme performant.

Même si ce temps de calcul est acceptable pour certaines applications car on génère les clés RSA une seule fois pour une application donnée, ceci n'est pas satisfaisant pour les services de téléphonie mobile (GSM par exemple) car cette opération se renouvelle à chaque changement de carte SIM et qu'un plus grand nombre de clés doit être prévu pour répondre aux besoins de différentes applications.

Du fait d'un besoin en ressources de calcul important, les clés sont toujours créées durant la phase de personnalisation à partir des exposants publics et fournis par les différentes entités fournisseur de service. Cette étape de calcul ne peut pas être mise en œuvre ultérieurement car elle paralyserait le fonctionnement de l'objet.

De façon pratique ce calcul n'est pas mis en œuvre par la carte. En effet, ce calcul est long et il pourrait ralentir la phase de personnalisation, de plus sa durée est variable et elle pourrait se révéler incompatible avec les procédés de personnalisation des cartes à puce.

D'autre part, cette solution présente toujours le second inconvénient de la solution précédente à savoir la nécessité de ressource mémoire.

La présente invention a pour but de résoudre ces problèmes.

Plus précisément l'invention a pour objectif de résoudre le problème de lourdeur du calcul lié à la gestion de génération de clés ainsi que le problème de manque de flexibilité dû au stockage initial et définitif d'un nombre important de clés et de certificats en phase de personnalisation.

A cette fin, un objet de la présente invention concerne un procédé de génération de clés électroniques d pour procédé de cryptographie à clé publique au moyen d'un dispositif électronique, principalement  
5 caractérisé en ce qu'il comprend deux étapes de calcul dissociées :

Etape A

- 1) Calcul de couples de nombres premiers  $(p,q)$  ou de valeurs représentatives de couples de  
10 nombres premiers, ce calcul étant indépendant de la connaissance du couple  $(e,l)$  dans lequel  $e$  est l'exposant public et  $l$  la longueur de la clé du procédé de cryptographie,  $l$  étant également la longueur du module  $N$  dudit  
15 procédé,
- 2) Stockage des couples ou des valeurs ainsi obtenus ;

Etape B

Calcul de la clé  $d$  à partir des résultats de  
20 l'étape A et de la connaissance du couple  $(e,l)$ .

Selon une première variante, l'étape A-1) consiste à calculer des couples de nombres premiers  $(p,q)$  sans connaissance de l'exposant public  $e$  ni de la longueur  $l$   
25 de la clé, en utilisant un paramètre  $\Pi$  qui est le produit de petits nombres premiers. De cette manière couple  $(p,q)$  obtenu à l'étape A, a une probabilité maximale de pouvoir correspondre à un futur couple  $(e,l)$  et permettra de calculer une clé  $d$  lors de la  
30 mise en œuvre de l'étape B.

Selon une autre variante dépendante de la variante précédente, le calcul A-1) tient compte en plus du fait que  $e$  a une forte probabilité de faire partie de l'ensemble  $\{3, 17, \dots, 2^{16+1}\}$ , on utilise pour cela dans le

calcul de l'étape A, une graine  $\sigma$  qui permet de calculer non pas des couples  $(p,q)$  mais une valeur représentative appelée image des couples  $(p,q)$ .

5 Le stockage A-2) consiste alors à mémoriser cette image. Ceci permet de gagner de la place mémoire puisqu'une image est plus petite qu'un nombre premier  $p$  ou  $q$  par exemple 32 octets comparés à 128 octets.

Selon une troisième variante on effectue un calcul de couples  $(p,q)$  pour différents couples  $(e,l)$  probables. De façon pratique le paramètre  $\Pi$  va contenir les valeurs usuelles de  $e$  par exemple 3, 17.

Selon une quatrième variante l'étape A-1) comprend une opération de compression des couples  $(p,q)$  calculés et l'étape A-2) consiste alors à stocker les valeurs compressées ainsi obtenues.

L'étape B comprend la vérification des conditions suivantes pour un couple  $(e, \ell)$  donné:

- (i)  $p-1$  et  $q-1$  premiers avec  $e$  et,
- (ii)  $N = p \cdot q$  un nombre entier de longueur  $\ell$ .

20

Selon un mode de réalisation préféré, l'étape A-1) comprend la génération d'un nombre premier  $q$ , le choix d'une limite inférieure  $B_0$  pour la longueur  $\ell_0$  de ce nombre premier à générer telle que  $\ell_0 \geq B_0$  par exemple

25  $B_0 = 256$  bits, et elle comprend en outre les sous-étapes suivantes :

1) -calculer des paramètres  $v$  et  $w$  à partir des relations suivantes et les mémoriser:

30 
$$v = \sqrt{2^{2\ell_0} - 1} / \Pi$$

$$w = 2^{\ell_0} / \Pi$$

dans lesquelles  $\Pi$  est mémorisé et correspond au produit des  $f$  plus petits nombres premiers,  $f$  étant choisi de manière telle que  $\Pi \leq 2^{B_0}$ ,

2)-choisir un nombre  $j$  dans l'intervalle des nombres entiers  $\{v, \dots, w-1\}$  et calculer  $\ell = j \Pi$  ;

3)-choisir et enregistrer un nombre premier  $k$  de longueur courte par rapport à la longueur d'une clé RSA dans l'intervalle des nombres entiers  $\{0, \dots, \Pi-1\}$ ,  
 5  $(k, \Pi)$  étant co-premiers, ;

4)-calculer  $q = k + \ell$ ,

5)-vérifier que  $q$  est un nombre premier, si  $q$  n'est pas un nombre premier alors :

10 a) prendre une nouvelle valeur pour  $k$  au moyen de la relation suivante :

$k = a k \pmod{\Pi}$  ;  $a$  appartenant au groupe multiplicatif  $Z^*_\Pi$  des nombres entiers modulo  $\Pi$ ;

b) réitérer à partir de la sous-étape 4).

15

Avantageusement l'étape B comprend, pour un couple  $(p, q)$  obtenu à l'étape A, et un couple  $(e, l)$  donné :

- La vérification des conditions suivantes :

(i)  $p-1$  et  $q-1$  premiers avec  $e$  et,

20 (ii)  $N = p * q$  un nombre entier de longueur  $\ell$ ,

- Si le couple  $(p, q)$  ne répond pas à ces conditions :

- Choix d'un autre couple et réitération de la vérification jusqu'à ce qu'un couple convienne,

25 - Calcul de la clé  $d$  à partir du couple  $(p, q)$  obtenu à l'issue de cette vérification.

L'invention a également pour objet, un objet sécurisé portatif apte à générer des clés électroniques  
 30 d'un algorithme de cryptographie de type RSA, caractérisé en ce qu'il comprend au moins :

- Des moyens de communication pour recevoir au moins un couple  $(e, l)$ ,



- Une mémoire pour stoker les résultats d'une étape A consistant à :

Calculer des couples de nombres premiers  $(p,q)$  ou de valeurs représentatives de couples de nombres premiers, ce calcul étant indépendant de la connaissance du couple  $(e,l)$  dans lequel  $e$  est l'exposant public et  $l$  la longueur de la clé du procédé de cryptographie,  $l$  étant également la longueur du module  $N$  dudit procédé,

- Un programme pour mettre en œuvre une étape B consistant à :

Calculer d'une clé  $d$  à partir des résultats de l'étape A et de la connaissance d'un couple  $(e,l)$ ,

L'objet sécurisé portatif comprend en outre un programme pour la mise en œuvre de l'étape A, les étapes A et B étant dissociées dans le temps.

L'objet sécurisé portatif pourra être constitué par une carte à puce.

D'autres particularités et avantages de l'invention apparaîtront clairement à la lecture de la description qui est donnée ci-après à titre d'exemple non limitatif et en regard de la figure unique représentant un schéma d'un système de mise en œuvre du procédé.

La suite de la description est faite dans le cadre de l'application de l'invention à un objet portatif de type carte à puce et pour simplifier l'expression on parlera de carte à puce.

Selon le procédé proposé la génération de clés se fait en deux étapes dissociées.

La première Etape A comporte un calcul de couples de nombres premiers  $(p,q)$  ou de valeurs représentatives de couples de nombres premiers appelée image.

Les couples  $(p,q)$  obtenus sont stockés.

5 Ce calcul est lourd et il est d'autant plus lourd si on utilise un algorithme de génération de nombres premiers classique.

Il est proposé ici que ce calcul soit effectué de manière indépendante de la connaissance du couple  
10  $(e,l)$ .

Comme cela va être détaillé dans la suite un mode de réalisation préféré pour mettre en œuvre cette étape permet d'alléger les calculs et de limiter la place mémoire nécessaire pour le stockage des couples  $(p,q)$   
15 obtenus en stockant une image de ces couples.

La deuxième Etape B comporte le calcul à proprement parler de la clé  $d$  à partir des résultats de l'étape A et de la connaissance du couple  $(e,l)$ .

Ce calcul comprend, pour un couple  $(p,q)$  obtenu à  
20 l'étape A, et un couple  $(e,l)$  donné :

- La vérification des conditions suivantes :
  - (i)  $p-1$  et  $q-1$  premiers avec  $e$  et,
  - (ii)  $N = p \cdot q$ , ce nombre doit être un nombre entier et de longueur  $l$ ,
- 25 - Si un couple  $(p,q)$  ne répond pas à ces conditions, on choisit un autre couple et on réitère de la vérification jusqu'à ce qu'un couple convienne parmi les couples obtenus lors de l'étape A.

- On peut procéder alors au calcul de la clé  $d$  à partir du couple  $(p,q)$  obtenu à l'issue de cette  
30 vérification.

La première étape qui correspond à un calcul relativement lourd par rapport à la deuxième étape, peut être exécutée par un autre organe que la carte à

puce par exemple par un serveur. Dans ce cas, les résultats du calcul de cette première étape pourront être chargés sur une carte à puce au moment de la personnalisation.

5           Le calcul de l'étape A peut également être fait par la carte elle-même à un instant quelconque qui ne gêne pas l'utilisateur de cette carte. Par exemple, ce calcul peut être fait lors de la personnalisation de la carte ou plus tard.

10           De façon pratique, lors de l'utilisation de la carte, pour obtenir un service, si une clé privée est nécessaire, alors la clé publique est fournie par le fournisseur de service (éventuellement à distance si elle n'est pas déjà stockée dans la carte) afin de  
15           générer la clé privée. Cette étape de génération (étape B de calcul) est effectuée de manière rapide par la carte.

          On voit donc que de nouvelles applications qui nécessitent le calcul d'une clé privée peuvent être  
20           prévues pour une carte.

          On voit également qu'il n'y a pas besoin d'associer un certificat aux couples  $(p,q)$  car ils ne sont pas associés à une clé privée.

          Ainsi, la génération d'une clé privée peut être  
25           faite à bord c'est à dire par la carte elle-même avec un gain d'un facteur 10 en temps d'exécution par rapport aux procédés de génération de clés connus à ce jour.

30           On va décrire dans ce qui suit un mode préféré de réalisation pour la mise en œuvre de l'étape A. Ce mode de réalisation est particulièrement avantageux pour la mise à bord d'une carte à puce car il permet

d'optimiser à la fois la place mémoire mais aussi le temps de calcul.

5 Tout d'abord, afin de s'assurer que  $N=p*q$  est un entier de  $l$ -bit, on choisit  $p$  appartenant à l'intervalle :

$$\left[ \sqrt{2^{2(l-l_0)-1}}, 2^{l-l_0} - 1 \right]$$

Et  $q$  appartenant à l'intervalle :

10

$$\left[ \sqrt{2^{2l_0-1}}, 2^{l_0} - 1 \right]$$

Pour  $l_0$  compris entre 1 et  $l$ .

15 Ainsi  $\min(p)\min(q)$  est compris entre  $2^{l_0}-1$  et  $N$ , et  $\max(p)\max(q)$  est compris entre  $N$  et  $2^l$  comme cela est demandé.

De cette façon, la condition ii) ci-dessus mentionnée se réduit à rechercher des nombres premiers dans l'intervalle :

20

$$\left[ \sqrt{2^{2l_0-1}}, 2^{l_0} - 1 \right]$$

25 La solution proposée exploite le paramètre  $\Pi$ . Ce paramètre  $\Pi$  est le produit de petits nombres premiers dans lequel on peut trouver notamment 3, 17,  $2^{16+1}$ , nombres premiers généralement utilisés comme exposants publics. Ainsi, la probabilité pour qu'un couple  $(p,q)$  corresponde à un futur couple  $(e,l)$  donné, déjà très élevée, augmente encore lorsque  $\Pi$  comporte de telles valeurs.

30

On choisit les  $f$  plus petits nombres premiers,  $f$  étant choisi de manière telle que  $\Pi_i p_i \leq 2B_0$ ,  $B_0$  est la

borne inférieure choisie pour  $l_0$ . par exemple on peut choisir  $B_0$  égal à 256 bits.

$\Pi$  est égal au produit : 2.3....191 et est inférieur à  $2^{256}$ .

5 On peut alors mémoriser cette valeur  $\Pi$  dans la carte par exemple comme une constante dans la mémoire morte de programme.

La première phase du procédé consiste à générer et à enregistrer un nombre premier  $k$  de longueur courte par rapport à la longueur d'une clé RSA dans l'intervalle des nombre entiers  $\{0, \dots, \Pi-1\}$ , ( $k, \Pi$ ) étant copremiers, c'est à dire n'ayant pas de facteur commun.

15 La deuxième phase consiste ensuite à partir de ce nombre  $k$  à construire le premier candidat  $q$  qui satisfait la condition d'être copremier avec  $\Pi$ .

Si ce premier candidat ne satisfait pas cette condition, alors il est mis à jour c'est à dire qu'un autre candidat est choisi jusqu'à ce qu'une valeur de  $q$  satisfaisant à la condition soit trouvée.

20 On va présenter dans la suite les différentes étapes de l'algorithme de génération d'un nombre premier entrant dans le calcul d'une clé RSA selon l'invention.

25 L'algorithme proposé fonctionne quelle que soit la longueur  $l_0$  donnée pour le nombre premier  $q$  qui doit être généré.

La génération du nombre premier  $p$  est identique, il suffit de remplacer  $q$  par  $p$  dans les étapes qui vont être développées et de remplacer  $l_0$  par  $l-l_0$ .

30 Après avoir fixé la limite  $B_0$ , on calcule les nombres premiers uniques  $v$  et  $w$  satisfaisant les conditions suivantes:

$$\begin{aligned} \sqrt{2^{2^{\ell_0-1}}} \leq v\Pi \leq \sqrt{2^{2^{\ell_0-1}}} + \Pi, \\ 2^{\ell_0} - \Pi \leq w\Pi \leq 2^{\ell_0} \end{aligned}$$

5 Ceci, se traduit par le calcul de  $v$  et  $w$  par les relations suivantes :

$$\begin{aligned} v &= \sqrt{2^{2^{\ell_0-1}}} / \Pi \\ w &= 2^{\ell_0} / \Pi \end{aligned}$$

10 Puis après avoir pris  $k$  appartenant au groupe multiplicatif  $Z^*\Pi$  des nombres entiers modulo  $\Pi$ , on construit le premier candidat  $q$  tel que,

$q = k + j\Pi$  pour tout  $j$  appartenant à l'intervalle  $[v, w-1]$  .

15 Comme justement  $k$  appartient à  $Z^*\Pi$ , la probabilité pour avoir un premier candidat  $q$  premier, est élevée. Si ce n'est pas le cas, on met à jour  $k$  en prenant  $k$  égal à  $ak \pmod{\Pi}$ ,  $a$  appartenant au groupe  $Z^*\Pi$  et on réitère jusqu'à trouver une valeur de  $q$  correspondant à un nombre premier.

20 Une manière de tester la primalité d'un nombre est par exemple d'utiliser le test de Rabin-Miller.

Les différentes étapes de l'algorithme proposé sont précisément les suivantes :

25 1) -calculer des paramètres  $v$  et  $w$  à partir des relations suivantes et les mémoriser:

$$\begin{aligned} v &= \sqrt{2^{2^{\ell_0-1}}} / \Pi \\ w &= 2^{\ell_0} / \Pi \end{aligned}$$

30 dans lesquelles  $\Pi$  est mémorisé et correspond au produit des  $f$  plus petits nombres premiers,  $f$  étant choisi de manière telle que  $\Pi \leq 2^{B_0}$ ,

2) -choisir un nombre  $j$  dans l'intervalle des nombres entiers  $\{v, \dots, w-1\}$  et calculer  $\ell = j\Pi$  ;

3) -choisir et enregistrer un nombre premier  $k$  de longueur courte par rapport à la longueur d'une clé RSA dans l'intervalle des nombres entiers  $\{0, \dots, \Pi-1\}$ ,  $(k, \Pi)$  étant co-premiers, ;

5 4) -calculer  $q = k + \ell$ ,

5) -vérifier que  $q$  est un nombre premier, si  $q$  n'est pas un nombre premier alors :

a) prendre une nouvelle valeur pour  $k$  au moyen de la relation suivante :

10  $k = a k \pmod{\Pi}$ ;  $a$  appartenant au groupe multiplicatif  $Z^*_{\Pi}$  des nombres entiers modulo  $\Pi$ ;

b) réitérer à partir de l'étape 4) ;

6) enregistrer  $a, k, j$  pour les utiliser afin de retrouver  $q$  et ensuite exploiter  $q$  pour l'utiliser lors d'un calcul ultérieur de génération d'une clé RSA.

Au lieu de stocker la valeur de  $q$  on va procéder avantageusement comme décrit dans la suite.

Une manière simple de mettre en œuvre cet algorithme peut consister pour chaque longueur de clé RSA envisagée, de stocker les valeurs de  $k$  et  $j$  de manière à re construire  $q$ .

Plutôt que de choisir un nombre aléatoire  $j$  comme indiqué à l'étape 2) un autre mode de réalisation peut consister à construire  $j$  à partir d'un nombre aléatoire court.

On prend par exemple un nombre de longueur 64-bit, que l'on désigne par graine et que l'on dénote  $\sigma$ . Cette graine est alors prise comme valeur d'entrée d'un générateur de nombres pseudo-aléatoires PRNG, lequel va permettre de générer  $j$ .

$j$  est alors défini comme  $\text{PRNG}_1(\sigma) \pmod{(w-v)+v}$ .

Ce mode d'exécution permet de réduire considérablement les besoins en place mémoire car il n'y a à stocker que les valeurs de  $\sigma$  et de  $k$  en mémoire

EEPROM. La valeur de  $\Pi$  est en mémoire morte (dans le programme de calcul).

On peut encore réduire les besoins en place mémoire en constatant que : si  $k_{(o)}$  est la première valeur de  $k$  appartenant au groupe  $Z^*[\Pi]$ , alors, les nombres premiers  
5 générés ont la forme :

$$q = a^{f-1} k_{(o)} \bmod \Pi + j \Pi$$

$f$  étant le nombre d'échec du test de l'étape 4).

Cette valeur  $k_{(o)}$  qui appartient au groupe  $Z^*[\Pi]$ , peut  
10 être facilement calculée à partir d'une graine aléatoire courte comme  $\sigma$  par exemple et en utilisant la fonction de Carmichael de  $\Pi^2$  dénotée  $\lambda(\Pi)$ .

En utilisant cette fonction on peut exprimer  $k_{(o)}$  par la relation suivante :

$$15 \quad k_{(o)} = [\text{PRNG}_2(\sigma) + b^{\text{PRNG}_3(\sigma)} (\text{PRNG}_2(\sigma)^{\lambda(\Pi)} - 1)] \pmod{\Pi}$$

$b$  étant un élément d'ordre  $\lambda(\Pi)$  appartenant à  $Z^*[\Pi]$ .

Ces deux modes d'exécution permettent de réduire les besoins en place mémoire puisqu'on ne va devoir  
20 stoker dans ce cas, que la valeur de la graine  $\sigma$  et différentes valeurs de  $f$  pour les longueurs désirées de clés.

Pour des clés RSA de modulo supérieur à 2048 bits, les expériences numériques qui ont été faites par les  
25 inventeurs montrent que  $f$  est égal à  $2^8$ . Ceci signifie que  $f$  peut être codé sur 1 byte soit 8 octets.

A titre d'exemple, pour générer des clés RSA de longueur allant de 512 à 2048 bits avec une granularité de 32 bits, il y a 49 longueurs de clé possibles. Il  
30 est donc nécessaire de stocker sur la carte un byte soit 8 octets correspondant à la valeur de  $\sigma$ . Il est également nécessaire de stocker les valeurs de  $f$  pour les nombres premiers  $p$  et  $q$  soit  $2 \cdot 49 = 98$  octets. Ceci



fait au total 106 bytes soit 848 bits en mémoire EEPROM.

Un dernier mode d'exécution permettant de réduire la place mémoire, consiste à stocker dans le programme de calcul, c'est à dire en mémoire de programme, plusieurs valeurs de  $\Pi$  et les valeurs de  $\lambda(\Pi)$  correspondantes pour différentes longueurs de clés envisagées. On peut remarquer qu'une grande valeur de  $\Pi$  conduit aux plus petites valeurs pour  $f$ .

Le nombre premier  $q$  généré selon l'étape 4) par l'algorithme qui vient d'être décrit satisfait comme on l'a vu précédemment à la condition :

$$q = a^{f-1} k_{(o)} \bmod \Pi + j * \Pi$$

Si  $e$  divise  $\Pi$  on peut exprimer  $q$  par la relation suivante :

$$q = a^{f-1} k_{(o)} \bmod (e)$$

Afin que la condition i) énoncée au début de la description soit remplie, il faut choisir  $a$  tel que  $a=1 \pmod{e}$  et forcer  $k_{(o)}$  de manière à ce qu'il soit différent de  $1 \pmod{e}$ .

Ainsi le nombre premier  $q$  obtenu satisfait la relation  $q = k_{(o)}$  différent de  $1 \pmod{e}$ .

La génération du nombre premier  $p$  est identique,  $q$  est remplacé par  $p$  dans les étapes qui ont été développées et  $l_0$  par  $1-l_0$ .

Comme cela a été dit, le programme mettant en œuvre le procédé de la carte n'a pas besoin de connaître à priori l'exposant public  $e$ . Cet exposant peut donc être fourni à tout moment par une application chargée dans la carte.

Toutefois, on sait que pour la plupart des applications (plus de 95%), les valeurs de  $e$  utilisées sont les valeurs  $\{3, 17, 2^{16}+1\}$ .

5 Afin de couvrir le plus grand nombre d'applications, on va de façon préférentielle choisir  $a$  tel que  $a \equiv 1 \pmod{\{3, 17, 2^{16}+1\}}$  et forcer  $k_{(e)}$  différent de cette valeur :  $1 \pmod{\{3, 17, 2^{16}+1\}}$ .

10 On choisit par exemple comme candidat possible pour  $a$ , le nombre premier  $R = 2^{64} - 2^{32} + 1$  à condition que le plus grand commun diviseur de  $\Pi$  et de  $R$  soit égal à 1.

La condition requise pour  $k_{(e)}$  peut être obtenue par le théorème du reste chinois.

15 Comme cela a été dit une autre alternative peut consister pour l'étape A-1) à calculer des couples de nombres premiers  $(p, q)$  pour différents couples  $(e, l)$  probables.

20 En conclusion, l'invention propose un procédé en deux étapes dissociées, la deuxième étape très rapide par rapport aux solutions connues, peut être exécutée en temps réel. Ce procédé est également peu coûteux en place mémoire.

25 En outre, il n'y a pas de limite pour de nouvelles applications non prévues à la personnalisation de la carte.

## REVENDEICATIONS

1. Procédé de génération de clés électroniques d pour procédé de cryptographie à clé publique au moyen d'un dispositif électronique, principalement caractérisé en ce qu'il comprend deux étapes de calcul dissociées :

5

## Etape A

1) Calcul de couples de nombres premiers  $(p,q)$  ou de valeurs représentatives de couples de nombres premiers, ce calcul étant indépendant de la connaissance du couple  $(e,l)$  dans lequel  $e$  est l'exposant public et  $l$  la longueur de la clé du procédé de cryptographie,  $l$  étant également la longueur du module  $N$  dudit procédé,

10

15

2) Stockage des couples ou des valeurs ainsi obtenus ;

## Etape B

Calcul d'une clé  $d$  à partir des résultats de l'étape A et de la connaissance du couple  $(e,l)$ .

20

2. Procédé de génération de clés électroniques selon la revendication 1, caractérisé en ce que l'étape A-1) consiste à calculer des couples de nombres premiers  $(p,q)$  sans connaissance de l'exposant public  $e$  ni de la longueur  $l$  de la clé, en utilisant un paramètre  $\Pi$  qui est le produit de petits nombres premiers, de manière à ce que chaque couple  $(p,q)$  ait une probabilité maximale de pouvoir correspondre à un futur couple  $(e,l)$  et puisse permettre de calculer une clé  $d$ .

25

30

3. Procédé de génération de clés électroniques selon la revendication 2, caractérisé en ce que le

calcul de l'étape A-1) tient compte en plus du fait que  $e$  a une forte probabilité de faire partie de l'ensemble  $\{3, 17, \dots, 2^{16+1}\}$ , on utilise pour cela dans ce calcul une graine  $\sigma$  qui permet de calculer non pas des couples  
5 (p,q) mais une valeur représentative appelée image des couples (p,q).

4. Procédé de génération de clés électroniques selon la revendication 1 et 3, caractérisé en ce que le  
10 stockage A-2) consiste à mémoriser l'image des couples.

5. Procédé de génération de clés électroniques selon la revendication 1, caractérisé en ce que l'étape A-1) consiste à calculer des couples de nombres  
15 premiers (p,q) pour différents couples (e,l) probables.

6. Procédé de génération de clés électroniques selon les revendications 2 et 5, caractérisé en ce que le paramètre  $\Pi$  contient les valeurs usuelles de  
20 l'exposant public  $e$  par exemple 3, 17.

7. Procédé de génération de clés électroniques selon la revendications 1, caractérisé en ce que l'étape A-1) comprend une opération de compression des  
25 couples (p,q) calculés et l'étape A-2) consiste alors à stocker les valeurs compressées ainsi obtenues.

8. Procédé de génération de clés électroniques selon la revendication 1, caractérisé en ce que l'étape  
30 A-1) comprend la génération d'un nombre premier  $q$ , pour lequel on fixe une limite inférieure  $B_0$  pour la longueur  $\ell_0$  de ce nombre premier à générer, telle que  $\ell_0 \geq B_0$  par exemple  $B_0 = 256$  bits, et en ce qu'elle comprend les sous étapes suivantes :

1) -calculer des paramètres  $v$  et  $w$  à partir des relations suivantes et les mémoriser:

$$v = \sqrt{2^{2\ell_0} - 1} / \Pi$$

$$w = 2^{\ell_0} / \Pi$$

dans lesquelles  $\Pi$  est mémorisé et correspond au produit des  $f$  plus petits nombres premiers,  $f$  étant choisi de manière telle que  $\Pi \leq 2^{B_0}$ ,

2) -choisir un nombre  $j$  dans l'intervalle des nombres entiers  $\{v, \dots, w-1\}$  et calculer  $\ell = j \Pi$  ;

3) -choisir et enregistrer un nombre premier  $k$  de longueur courte par rapport à la longueur d'une clé RSA dans l'intervalle des nombres entiers  $\{0, \dots, \Pi-1\}$ ,  $(k, \Pi)$  étant co-premiers, ;

4) -calculer  $q = k + \ell$ ,

5) -vérifier que  $q$  est un nombre premier, si  $q$  n'est pas un nombre premier alors :

a) prendre une nouvelle valeur pour  $k$  au moyen de la relation suivante :

$k = a k \pmod{\Pi}$  ;  $a$  appartenant au groupe multiplicatif  $Z^*_\Pi$  des nombres entiers modulo  $\Pi$ ;

b) réitérer à partir de l'étape 4) ;

9. Procédé de génération de clés électroniques selon les revendications 3 et 8, caractérisé en ce que les nombres  $j$  et  $k$  peuvent être générés à partir de la graine  $\sigma$  stockée en mémoire.

10. Procédé de génération de clés électroniques selon la revendication 8, caractérisé en ce que le nombre premier  $p$  est généré en réitérant toutes les sous étapes précédentes en remplaçant  $q$  par  $p$  et en remplaçant  $\ell_0$  par  $\ell - \ell_0$ .

11. Procédé de génération de clés électroniques selon l'une quelconque des revendications précédentes, caractérisé en ce que :

5 L'étape B comprend, pour un couple  $(p,q)$  obtenu à l'étape A, :

- La vérification des conditions suivantes :

(i)  $p-1$  et  $q-1$  premiers avec  $e$  donné et,

(ii)  $N = p \cdot q$  un nombre entier de longueur  $l$  donnée,

10 - Si le couple  $(p,q)$  ne répond pas à ces conditions :

- Choix d'un autre couple et réitération de la vérification jusqu'à ce qu'un couple convienne,

15 - Calcul de la clé  $d$  à partir du couple  $(p,q)$  obtenu.

12. Objet sécurisé portatif apte à générer des clés électroniques d'un algorithme de cryptographie de type RSA, caractérisé en ce qu'il comprend au moins :

20 - Des moyens de communication pour recevoir au moins un couple  $(e,l)$ ,

- Une mémoire pour stocker les résultats d'une étape A consistant à :

25 Calculer des couples de nombres premiers  $(p,q)$  ou de valeurs représentatives de couples de nombres premiers, ce calcul étant indépendant de la connaissance du couple  $(e,l)$  dans lequel  $e$  est l'exposant public et  $l$  la longueur de la clé du procédé de cryptographie,  $l$  étant également la  
30 longueur du module  $N$  de ce  $p$ ,

- Un programme pour mettre en œuvre une étape B consistant à :

Calculer une clé  $d$  à partir des résultats de l'étape A et de la connaissance d'un couple  $(e,l)$ ,

13. Objet sécurisé portatif selon la revendication  
12, caractérisé en ce qu'il comprend en outre un  
programme pour la mise en œuvre de l'étape A, les  
5 étapes A et B étant dissociées dans le temps.

14. Objet sécurisé portatif selon la revendication  
13, caractérisé en ce que le programme de mise en œuvre  
de l'étape A met en œuvre les sous-étapes :

1) -calculer des paramètres  $v$  et  $w$  à partir des  
relations suivantes et les mémoriser:

$$v = \sqrt{2^{2\ell_0} - 1} / \Pi$$

$$w = 2^{\ell_0} / \Pi$$

15 dans lesquelles  $\Pi$  est mémorisé et correspond au  
produit des  $f$  plus petits nombres premiers,  $f$  étant  
choisi de manière telle que  $\Pi \leq 2^{B_0}$ ,  $B_0$  est une limite  
inférieure fixée pour la longueur  $\ell_0$  du nombre premier à  
générer telle que  $\ell_0 \geq B_0$  par exemple  $B_0 = 256$  bits,

2) -choisir un nombre  $j$  dans l'intervalle des  
nombres entiers  $\{v, \dots, w-1\}$  et calculer  $\ell = j \Pi$  ;

3) -choisir et enregistrer un nombre premier  $k$  de  
longueur courte par rapport à la longueur d'une clé RSA  
dans l'intervalle des nombres entiers  $\{0, \dots, \Pi-1\}$ ,  
25  $(k, \Pi)$  étant co-premiers, ;

4) -calculer  $q = k + \ell$ ,

5) -vérifier que  $q$  est un nombre premier, si  $q$   
n'est pas un nombre premier alors :

a) prendre une nouvelle valeur pour  $k$  au moyen de  
30 la relation suivante :

$k = a k \pmod{\Pi}$  ;  $a$  appartenant au groupe  
multiplicatif  $Z^*_\Pi$  des nombres entiers modulo  $\Pi$ ;

b) réitérer à partir de l'étape 4).

15. Objet sécurisé portatif selon la revendication 12 ou 13 ou 14, caractérisé en ce qu'il est constitué par une carte à puce.



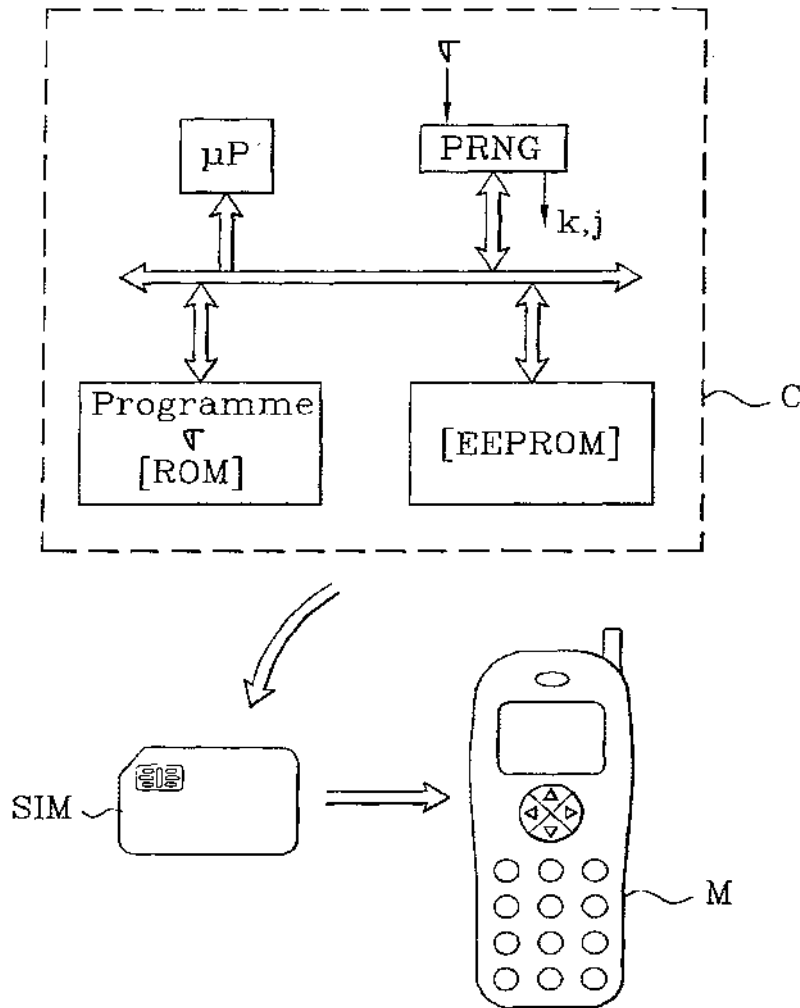


Figure unique

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
23 September 2004 (23.09.2004)

PCT

(10) International Publication Number  
WO 2004/081706 A2

(51) International Patent Classification<sup>7</sup>: G06F

(21) International Application Number: PCT/SG2004/000024

(22) International Filing Date: 27 January 2004 (27.01.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:  
2003901095 11 March 2003 (11.03.2003) AU

(71) Applicant (for US only): DIGISAFE PTE LTD [SG/SG];  
100 Jurong East St 21, Singapore 609602 (SG).

(72) Inventors; and

(75) Inventors/Applicants (for US only): CHOW, Andrew [SG/SG]; c/o Digisafe Pte Ltd, 100 Jurong East St 21, Singapore 609602 (SG). LEE, Ser, Yen [SG/SG]; c/o Digisafe Pte Ltd, 100 Jurong East St 21, Singapore 609602

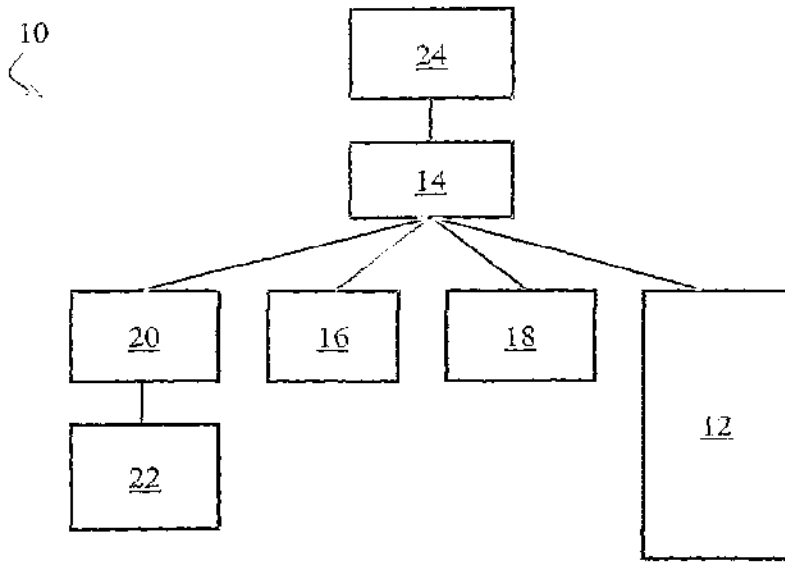
(SG). LAU, Puay, Hui [SG/SG]; c/o Digisafe Pte Ltd, 100 Jurong East St 21, Singapore 609602 (SG). CHIA, Boon, Quee [SG/SG]; c/o Digisafe Pte Ltd, 100 Jurong East St 21, Singapore 609602 (SG). TAN, Teck, Weng, Paul [SG/SG]; c/o Digisafe Pte Ltd, 100 Jurong East St 21, Singapore 609602 (SG). NG, Chee, We [SG/SG]; c/o Digisafe Pte Ltd, 100 Jurong East St 21, Singapore 609602 (SG). SOO, Hin, Meng, Timothy [SG/SG]; c/o Digisafe Pte Ltd, 100 Jurong East St 21, Singapore 609602 (SG). GATTAMENI, Venkateswara, Rao [SG/SG]; c/o Digisafe Pte Ltd, 100 Jurong East St 21, Singapore 609602 (SG). LOO, Whye, Ho, Jamez [SG/SG]; c/o Digisafe Pte Ltd, 100 Jurong East St 21, Singapore 609602 (SG).

(74) Agent: SIM, Yuan, Meng, Andrew; Shook Lin & Bok, 1 Robinson Road, #18-00 AIA Tower, Singapore 048542 (SG).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KI, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD,

[Continued on next page]

(54) Title: METHOD AND APPARATUS FOR CONTROLLING THE PROVISION OF DIGITAL CONTENT



(57) Abstract: An apparatus for controlling the provision of digital content, comprising a data storage device controller for receiving a data storage device on which is provided the content, an authentication data storage device for storing authentication data, a data port connectable to a host device so that the apparatus can be placed into electronic communication with the host device, and a communications hub to mediate electronic communication between the data storage device controller, the authentication data storage device and the data port, wherein the apparatus is configured to permit content provided on the data storage device to be outputted from the data port according to the authentication data.

WO 2004/081706 A2



MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

TR), OAPI (BI, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**(84) Designated States** (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GII, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK,

**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.

- 1 -

METHOD AND APPARATUS FOR CONTROLLING THE PROVISION  
OF DIGITAL CONTENT

FIELD OF THE INVENTION

5 The present invention relates to a digital security method and apparatus, of particular but by no means exclusive application in controlling the distribution of electronic content such as software (and, in one particular example, software drivers), the distribution of digital content or  
10 media with copy protection, digital personal identification devices (typically carrying personal identity and other data), data management and portable devices for the secure storage of electronic content (such as data or software).

15

BACKGROUND OF THE INVENTION

Software including software drivers are presently commonly distributed with corresponding hardware on computer readable media such as CD-ROM, or over the Internet.  
20 These approaches, however, require the provision of such media or an Internet connection, both restrictions on the portability of the hardware.

Currently techniques exist for preventing the copying of  
25 digital content on music CDs, but few particular effective approaches exist for digital media such as floppy diskettes, zip diskettes, CD-ROMs and USB-flash devices.

In the field of smart cards and other devices for storing  
30 personal data or for data management, techniques such as the use of secret keys and digital certificates are presently employed to identify a person's identity. Personal Digital Assistants (PDAs) carry personal information but are not generically designed to prove a  
35 person's identity. No such device exists that combines the storage of a person's identity with personal information such as electronic mail.

- 2 -

There also exist a number of mass storage USB tokens, including that of Trek Technology (Singapore) Pte Ltd as described in WO 01/61692. Further, WO 00/42491 (Rainbow Technologies Inc) describes a cryptographic USB token.

Existing approaches for the portable secure storage of digital data also include the encryption of files on diskettes.

10

#### SUMMARY OF THE INVENTION

The present provides, in a first broad aspect, an apparatus for controlling the provision of digital content, comprising:

15

a data storage device controller for receiving a data storage device on which is provided said content;

an authentication data storage device for storing authentication data;

20

a data port connectable to a host device so that said apparatus can be placed into electronic communication with said host device; and

25

a communications hub to mediate electronic communication between said data storage device controller, said authentication data storage device and said data port;

wherein said apparatus is configured to permit content provided on said data storage device to be outputted from said data port according to said authentication data.

30

Preferably said data storage device is a non-volatile data storage device. More preferably said data storage device is a flash memory device. In these embodiments, the data storage device controller is preferably a controller suitable for the respective device.

35

Thus, content (which could comprise software, audio,

- 3 -

video, personal or other information, etc.) can be provided on the data storage device (such as a flash memory device, for example a flash card), but only copied to the data port (and thence to, for example, a computer or a playback device) if a suitable correspondence exists between the authentication data and the content. For example, the content may be configured to be read from the data storage device only if a particular password, security key or digital certificate is provided: that password or security key would be stored as the authentication data on the authentication data storage device. The authentication data storage device could take any suitable form, as will be understood by those in the art, such as a smart card chip or a biometric device.

It should be understood, however, that the apparatus - though configured to permit content provided on said data storage device to be outputted from the data port according to said authentication data - may be configured so that this outputting is limited in a predetermined way. Thus, the data storage device may include a first storage portion for storing at least one software viewer or player for viewing or playing said content, and a second storage portion for storing said content, wherein said apparatus is configured to permit the accessing of said software viewer or player and of said content (such as by a computer when said apparatus is connected to that computer) such that said content can be viewed or played by means of said software viewer or player without allowing said content to be copied (such as to another device, storage medium or printer).

Preferably the apparatus includes a cryptographic processor that is operable to encrypt or decrypt said content by means of at least one cryptographic key stored in said authentication data storage device. The cryptographic key may comprise or be derived from the

- 4 -

authentication data.

Thus, the authentication data (whether comprising a  
password, a secret key and/or a digital certificate, or  
5 otherwise) can additionally be used for encryption and  
copy protection, and the apparatus is preferably operable  
to encrypt and/or decrypt said content on the basis of the  
authentication data (i.e. using the authentication data as  
a cryptographic key, or deriving a cryptographic key from  
10 the authentication data).

The authentication data storage device may also comprise a  
combination of secure microcontrollers and EEPROM chips.

15 The invention thereby provides an apparatus that can be  
used as both a mass storage token and as a cryptographic  
token (the latter preferably in the form of a  
cryptographic processor).

20 Preferably said communications hub comprises a Universal  
Serial Bus (USB) hub.

Preferably the data port comprises a USB connector.

25 In one embodiment, said content comprises software.

In another embodiment, said content comprises software  
device drivers.

30 Preferably said apparatus includes a communications port  
for connecting said apparatus to a hardware device  
associated with said content.

Alternatively, said apparatus is provided in a hardware  
35 device and in electronic communication with said hardware  
device.

- 5 -

Thus, the hardware device would typically be a hardware peripheral that the software device drivers will be working with. The data storage device is then used to contain the software drivers for the hardware device, or digital media, personal data and other data to be secured. The authentication data storage device can then also store unique secret keys for identifying the hardware device and/or for ensuring the authenticity and originality of the hardware.

10

In another embodiment, when the content comprises digital media for distribution with copy protection, the data storage device contains software portions or drivers for reading, displaying or playing said digital media.

15

Thus, these software components would typically be designed to prevent unauthorized duplication of the digital media stored on the data storage device by using techniques such as encryption and capturing operating system functions.

20

In one embodiment, further authentication data is stored on said data storage device.

25

Thus, for data management (such as of personal data), the content comprises software modules for the host device that are designed to be incorporated into software applications so that personal identity data, such as secret keys and digital certificates, may be stored in the data storage device as well as in the authentication data storage device. Other personal data, such as email and personal calendar, can be stored in the data storage device.

30

35

In another embodiment, for portable secure storage of digital data, the data storage device contains said digital data in encrypted form while the authentication



- 5 -

data storage device contains secret keys for the encryption.

5 In all the applications above, the data in the data storage device may be in clear or in encrypted form, depending on the application.

The present also provides, in a second broad aspect, a method for controlling the provision of digital content, comprising:

providing said content on a data storage device readable by means of a data storage device controller;

providing authentication data on an authentication data storage device;

15 placing said data storage device controller and authentication data storage device in data communication with a host device;

controlling the provision of said content to said host device according to at least said authentication data.

The present provides, in a third broad aspect, a method for controlling access to digital content, comprising:

25 providing said content on a computing or other electronic device;

providing authentication data and control software on an authentication apparatus comprising:

30 a control software storage device controller for receiving a control software storage device on which is provided control software;

an authentication data storage device for storing authentication data;

35 a data port connectable to said computing or other electronic device so that said apparatus can be placed into electronic communication with said computing or other electronic device; and

a communications hub to mediate electronic

- 7 -

communication between said authentication data storage device controller, said authentication data storage device and said data port;

wherein said apparatus is configured to permit said control software provided on said control software storage device storage device to be used to control application software on said computing or other electronic device according to said authentication data.

10 The electronic device could be a computer peripheral, such as a printer, a scanner or a digital camera. By this means, the software drivers can be distributed with the electronic device itself, rather than on a separate CD-ROM or the like.

15 Preferably the authentication apparatus includes a cryptographic processor that is operable to encrypt or decrypt said content by means of at least one cryptographic key stored in said authentication data storage device. More preferably, the cryptographic key  
20 comprises or is derived from the authentication data.

#### BRIEF DESCRIPTION OF THE DRAWINGS

In order that the present invention may be more clearly  
25 ascertained, preferred embodiments will now be described, by way of example, with reference to the accompanying drawing, in which:

Figure 1 is a schematic diagram of an apparatus for distributing content associated with a hardware device according to a preferred embodiment of the present  
30 invention, together with the hardware device;

Figure 2 is a schematic diagram of an apparatus for distributing software device drivers associated with a hardware device according to another preferred embodiment  
35 of the present invention, together with the hardware device;

Figure 3 is a schematic diagram of an apparatus

- 8 -

for distributing digital storage media with copy protection according to a further preferred embodiment of the present invention;

Figure 4 is a schematic diagram of an authentication apparatus for personal identity and data management and for portable secure storage of digital data according to another preferred embodiment of the present invention;

Figure 5 is a schematic diagram of a system for centrally programming and managing the apparatus of figure 4; and

Figure 6 is a perspective view of an example of the apparatus of figure 4.

#### 15 DETAILED DESCRIPTION OF THE DRAWINGS

An apparatus 10 for distributing digital content associated with a hardware device according to an embodiment of the present invention, together with the hardware device 12, is shown in figure 1.

20

The apparatus 10 comprises a Universal Serial Bus (USB) hub 14, an authentication device in the form of a smart card chip 16 or a biometric device 18, a flash controller 20 for reading flash memory 22 and a USB connector 24.

25

The authentication device 16,18 and the flash controller 20 communicate via USB hub 14 with a host device (not shown: typically a computer) by means of USB connector 24. The apparatus 10 is in fact incorporated within the hardware device 12 and connected thereto by means of a further USB connector (not shown) to the USB hub 14. The USB hub 14 in this embodiment will typically be the USB hub of the hardware device 12 itself.

35 The content on flash memory 22 (provided with the hardware device 12) to the host device is permitted only if the correct and corresponding authentication data is detected

- 9 -

on the authentication device 16,18.

Particular examples of applications of this approach are given below by reference to figures 2 to 4.

5

(1) Software Driver Distribution

Figure 2 is a schematic diagram of an apparatus 30 for distributing software device drivers associated with a hardware device according to an embodiment of the present invention, together with the hardware device 32.

The apparatus 30 comprises USB hub 34, an authentication device in the form of a smart card chip 36, a flash controller 40 for reading flash memory 42 and a USB connector 44. Flash memory 42 contains the content (here in the form of the software device drivers for hardware device 32) that are needed for the operating system of the host device (not shown, but connected at USB connector 44) to operate with the hardware device 32. The hardware device 32 could be a computer peripheral such as a printer, or scanner, or it could represent a smart card that itself acts as the authentication device.

The smart card chip 36 contains secret keys, etc., for establishing authenticity of the hardware device 32 and the software device driver: the software device driver performs authentication with the smart card chip 36 to ensure that the device driver has not been modified and the hardware device 32 is original.

30

(2) Digital Media Distribution with Copy Protection

Figure 3 is a schematic diagram of an apparatus 50 for distributing digital storage media with copy protection according to an embodiment of the present invention. The content in this example may be digitized music and video such as MP3 and MPEG or software packages.

35

- 10 -

The apparatus 50 comprises USB hub 54, an authentication device in the form of a smart card chip 56, a flash controller 60 for reading flash memory 62 and a USB connector 64. Flash memory 62 contains the content, in this example in the form of audio/video digital content to be distributed, and software applications to view, play and install the content on the host device (not shown, but connected at USB connector 64).

The content stored in the flash memory 62 is in encrypted form to prevent unauthorized duplication. Software viewers, players or installers also reside in the flash memory. The viewers, players and installers are written in a way that they only allow the media and applications to be viewed, played or installed, but do not allow them to be duplicated. Strong cryptographic protocols are used in these viewers, players and installers to prevent unauthorized duplication.

The smart card chip 56 contains secret keys or other parameters to prove the authenticity and originality of the media. Other information regarding the number of times a digital data has been accessed or the identity of the computer or player can be recorded in the smart card chip. This allows the number of times or the location the digital data or the software package has been accessed or installed can be restricted.

### (3) Personal Identity and Data Management and Portable Secure Storage of Digital Data

Figure 4 is a schematic diagram of an authentication apparatus 70 for personal identity and data management and for portable secure storage of digital data in the form of personal identity data according to an embodiment of the present invention. The authentication data is in the form of personal identity data such as digital certificates and passwords while the content (or personal data) could be

- 11 -

electronic mail, personal documents, passwords, and other data.

The apparatus 70 comprises USB hub 74, an authentication  
5 device in the form of a smart card chip 76, a flash  
controller 80 for reading flash memory 82 and a USB  
connector 84. Flash memory 82 contains the content which,  
as mentioned above, in this example is in the form of  
10 electronic mail, personal documents, passwords and other  
data.

The flash memory 82 is used to store these data in clear  
or encrypted form. The more sensitive data (together with  
the digital certificates or passwords for proving identity  
15 or the secret keys used to sign, encrypt and decrypt the  
data in the flash card 82) is securely stored in the smart  
card chip 76.

Digital certificates are used for secure computer  
20 applications such as secure email (S/MIME) and secure  
internet connection (Secure Socket Layer, SSL), for  
signing and encrypting email.

Figure 5 is a schematic diagram of a system 90 for  
25 centrally programming and managing the authentication  
apparatus 70 of figure 4, in use with such the  
authentication apparatus 70 and a computer network 92.

The system 90 comprises a central management system 94 and  
30 a programmer 96. The programmer 96 includes a USB port  
for connecting to the USB port of USB connector 84 of  
authentication apparatus 70, so that the system 90 can be  
used to program each such authentication apparatus 70 by  
installing in an authentication apparatus 70 keys  
35 belonging to each user.

The keys are held in a Public Key Depository 98, which

- 12 -

holds such keys for secure applications such as S/MIME. The Public Key Depository 98 is accessible by the central management system 94 by computer network.

5 The system 90 installs - into the flash memory 82 of each authentication apparatus 70 - installation and configuration programs for subsequently configuring the software applications on networked computers 100 (each running secure applications such as S/MIME) on computer  
10 network 92; a user can take an authentication apparatus that has been programmed in this manner (such as authentication apparatus 70') and use it to gain ready access to those applications on any of computers 100. This enables each user to use these applications easily  
15 without the necessity of a system administrator installing applications or performing configuration for the user. The user also does not need to carry along another medium (such as an installation disk), and is free to perform this installation at all the computers that the user is  
20 authorized to use.

This convenience for the user is enabled by the flash storage space, in addition to the smart card chip, the latter of which is responsible for the key storage.

25

This system thus reduces the complexity of deployment by incorporating all the installation program and information within the device itself.

30 Figure 6 is a perspective view of an example of an authentication apparatus 102 according to this embodiment (such as authentication apparatus 70 of figures 4 and 5). As is apparent in this figure, the authentication apparatus 102 includes a USB plug 104 (for plugging into a  
35 USB port) and a body 106 that encases the data storage and processing components of the apparatus. The apparatus 102 is designed to be hand-held, so it is of appropriate

- 13 -

dimensions and provided with finger grips 108 for ease of manipulation.

5 Thus, the present invention allows device drivers to be distributed together with the hardware device itself, and for a single architecture to be used for multiple applications.

10 Modifications within the scope of the invention may be readily effected by those skilled in the art. It is to be understood, therefore, that this invention is not limited to the particular embodiments described by way of example hereinabove.

15 In the claims that follow and in the preceding description of the invention, except where the context requires otherwise owing to express language or necessary implication, the word "comprise" or variations such as  
20 "comprises" or "comprising" is used in an inclusive sense, i.e. to specify the presence of the stated features but not to preclude the presence or addition of further features in various embodiments of the invention.



- 14 -

## CLAIMS:

1. An apparatus for controlling the provision of digital content, comprising:

5 a data storage device controller for receiving a data storage device on which is provided said content;

an authentication data storage device for storing authentication data;

10 a data port connectable to a host device so that said apparatus can be placed into electronic communication with said host device; and

15 a communications hub to mediate electronic communication between said data storage device controller, said authentication data storage device and said data port;

wherein said apparatus is configured to permit content provided on said data storage device to be outputted from said data port according to said authentication data.

20

2. An apparatus as claimed in claim 1, wherein said apparatus includes a cryptographic processor that is operable to encrypt or decrypt said content by means of at least one cryptographic key stored in said authentication data storage device.

25

3. An apparatus as claimed in claim 2, wherein said cryptographic key comprises or is derived from said authentication data.

30

4. An apparatus as claimed in any one of the preceding claims, wherein said data storage device includes a first storage portion for storing at least one software viewer or player for viewing or playing said content, and a second storage portion for storing said content, wherein said apparatus is configured to permit the accessing of said software viewer or player and of said content such

35

- 15 -

that said content can be viewed or played by means of said software viewer or player without allowing said content to be copied.

- 5 5. An apparatus as claimed in any one of the preceding claims, wherein said authentication data storage device comprises a combination of secure microcontrollers and EEPROM chips and said data storage device is a flash memory device.
- 10 6. An apparatus as claimed in any one of the preceding claims, wherein said communications hub comprises a Universal Serial Bus hub.
- 15 7. An apparatus as claimed in any one of the preceding claims, wherein said data port comprises a Universal Serial Bus connector.
- 20 8. An apparatus as claimed in any one of the preceding claims, wherein said content comprises software.
- 25 9. An apparatus as claimed in any one of preceding claims, wherein said content comprises software device drivers.
- 30 10. An apparatus as claimed in any one of preceding claims, including a communications port for connecting said apparatus to a hardware device associated with said content.
- 35 11. An apparatus as claimed in any one of preceding claims, wherein said apparatus is provided in a hardware device and in electronic communication with said hardware device.
12. An apparatus as claimed in claim 1, wherein said content comprises digital media for distribution with copy

- 16 -

protection, and said data storage device contains software portions or drivers for reading, displaying or playing said digital media.

5 13. An apparatus as claimed in claim 1, wherein further authentication data is stored on said data storage device.

14. A method for controlling the provision of digital content, comprising:

10 providing said content on a data storage device readable by means of a data storage device controller;

providing authentication data on an authentication data storage device;

15 placing said data storage device controller and authentication data storage device in data communication with a host device;

controlling the provision of said content to said host device according to at least said authentication data.

20

15. A method as claimed in claim 14, including encrypting or decrypting said content by means of at least one cryptographic key stored in said authentication data storage device.

25

16. A method as claimed in claim 15, wherein said cryptographic key comprises or is derived from said authentication data.

30 17. A method for controlling access to digital content, comprising:

providing said content on a computing or other electronic device;

35 providing authentication data and control software on an authentication apparatus comprising:

a control software storage device controller for receiving a control software storage device

- 17 -

on which is provided control software;

an authentication data storage device for storing authentication data;

5 a data port connectable to said computing or other electronic device so that said authentication apparatus can be placed into electronic communication with said computing or other electronic device; and

10 a communications hub to mediate electronic communication between said authentication data storage device controller, said authentication data storage device and said data port;

15 wherein said authentication apparatus is configured to permit said control software provided on said control software storage device to be used to control application software on said computing or other electronic device according to said authentication data.

18. A method as claimed in claim 17, wherein said  
20 authentication apparatus includes a cryptographic processor that is operable to encrypt or decrypt said content by means of at least one cryptographic key stored in said authentication data storage device.

25 19. A method as claimed in claim 18, wherein said cryptographic key comprises or is derived from said authentication data.

30

1/3

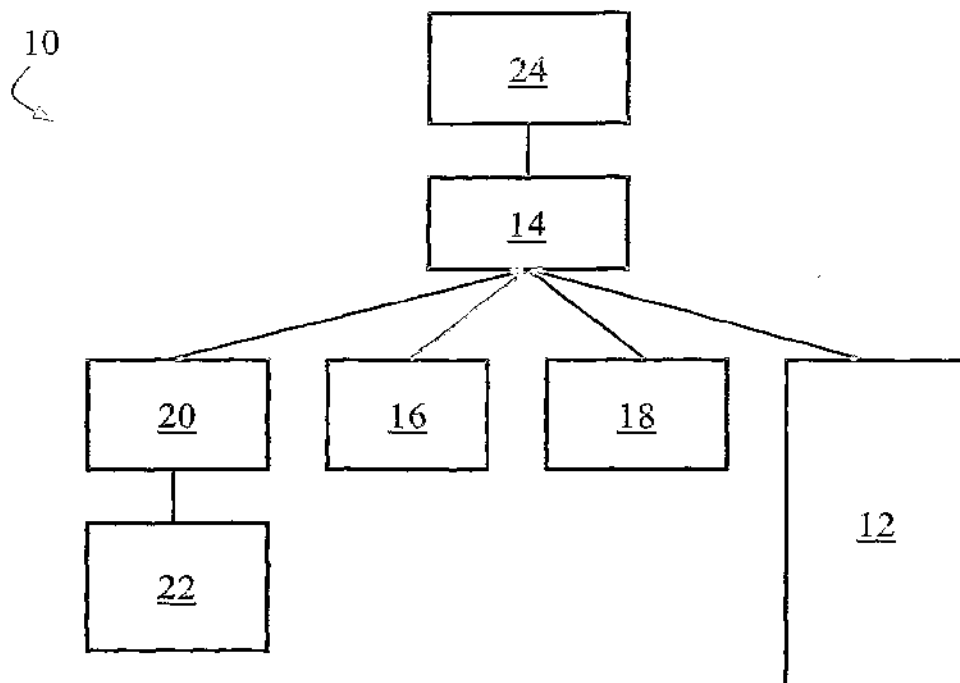


Figure 1

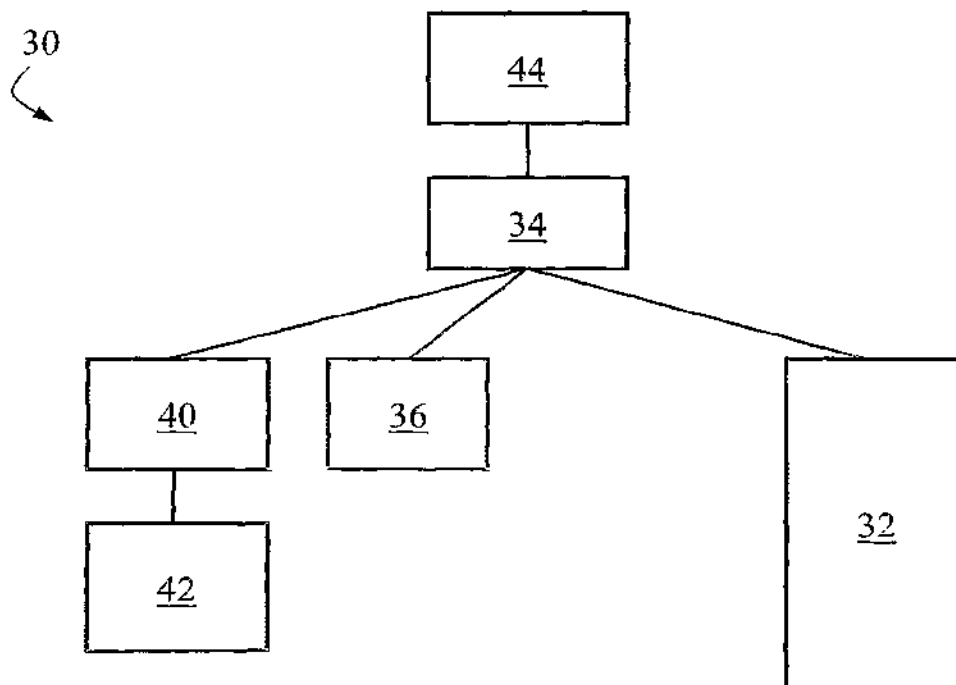


Figure 2

2/3

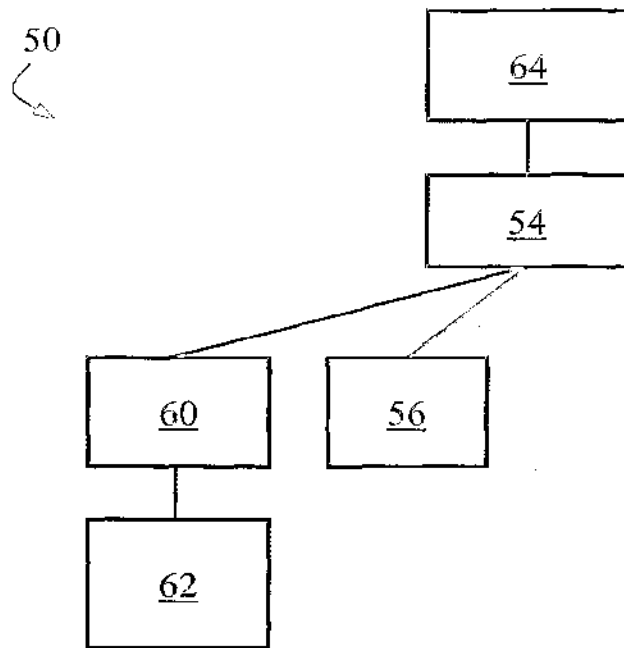


Figure 3

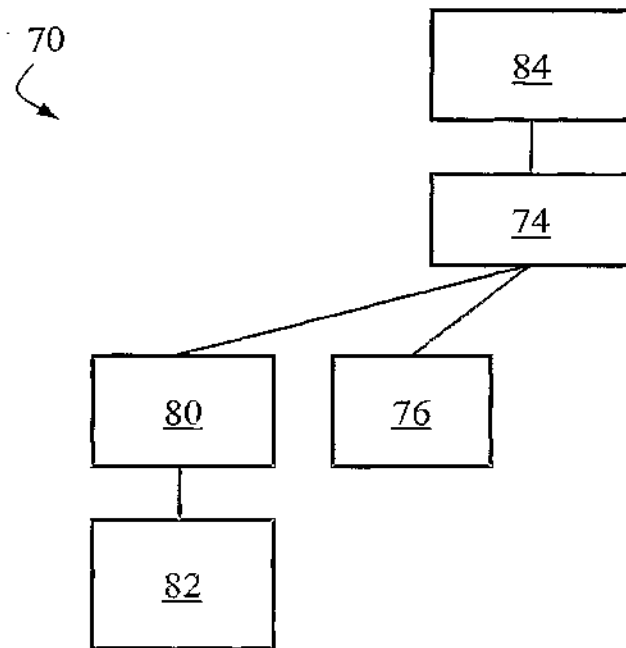


Figure 4

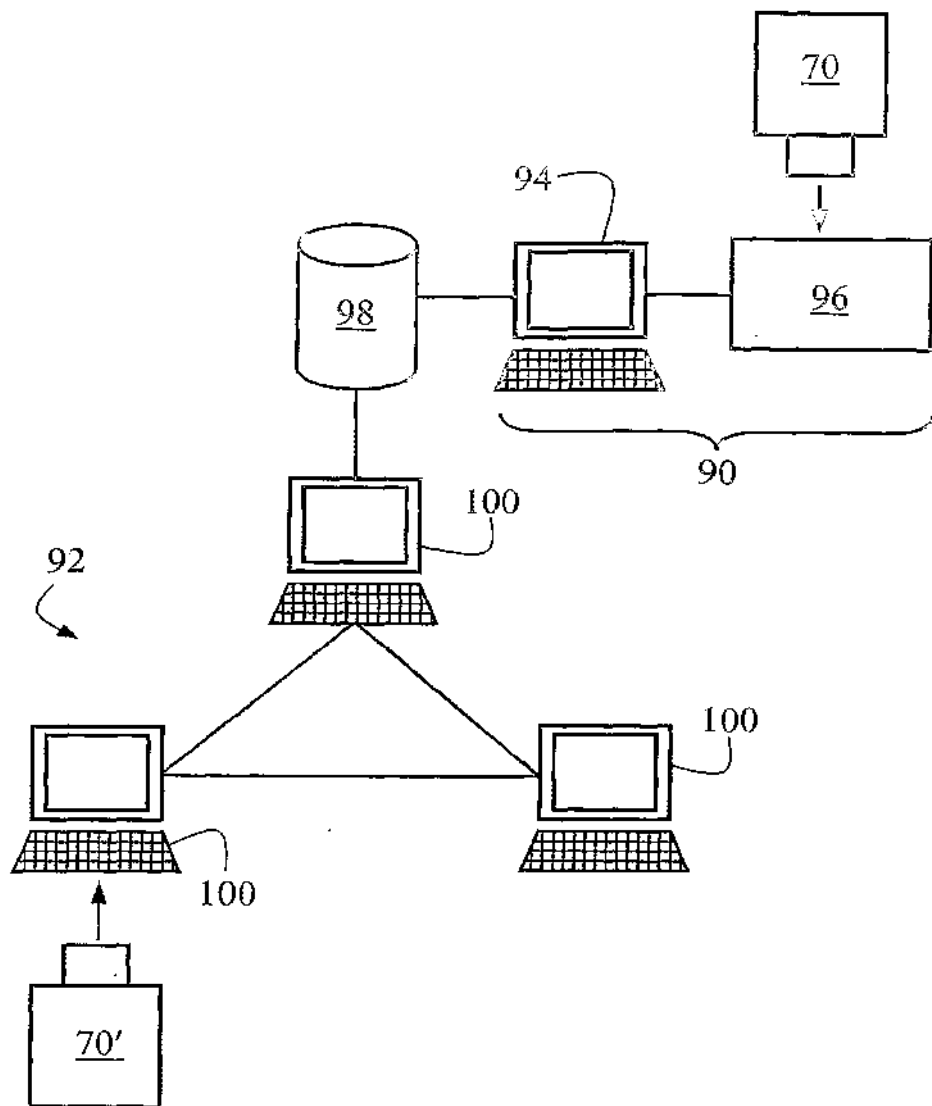


Figure 5

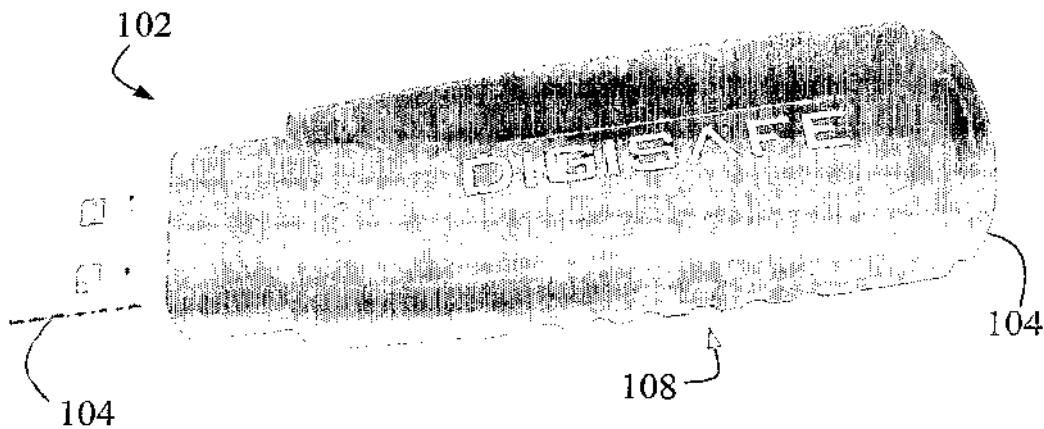


Figure 6

(19) World Intellectual Property Organization  
International Bureau



(43) International Publication Date  
23 September 2004 (23.09.2004)

PCT

(10) International Publication Number  
WO 2004/081769 A1

- (51) International Patent Classification<sup>7</sup>: G06F 1/00
- (21) International Application Number: PCT/IB2004/000738
- (22) International Filing Date: 12 March 2004 (12.03.2004)
- (25) Filing Language: English
- (26) Publication Language: English
- (30) Priority Data: 03290655.4 14 March 2003 (14.03.2003) EP
- (71) Applicant (for all designated States except US): AXALTO SA [FR/FR]; 36-38 rue de la Princesse, BP 45, F-78431 Louveciennes (FR).
- (71) Applicant (for MC only): SCHLUMBERGER MALCO INC [US/US]; 9800 Reisterstown, Owning Mills, Owning Mills, MD 21117 (US).
- (72) Inventor; and
- (75) Inventor/Applicant (for US only): AKKAR, Melodi-Laurent [FR/FR]; 17 Rue Lafouge, F-94250 Gentilly (FR).
- (74) Common Representative: SCHLUMBERGER SYSTEMES; C/O Patrice GUILLERM, 36-38 rue de la Princesse, BP 45, F 78431 Louveciennes (FR).

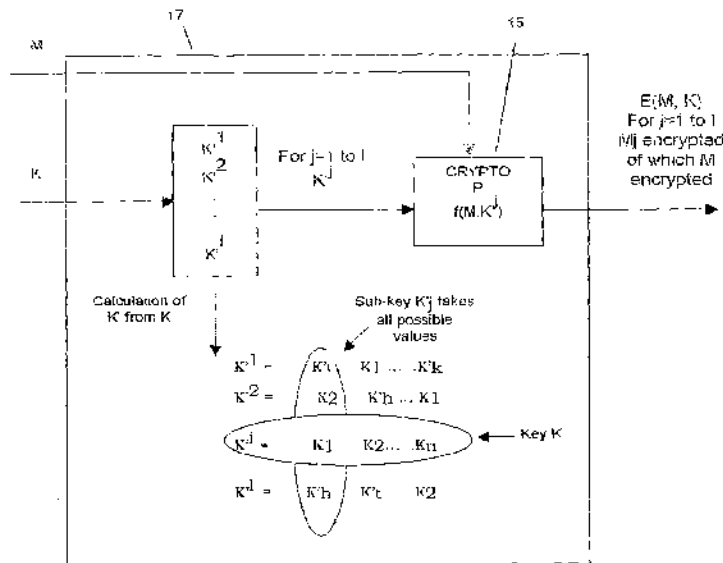
- (81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AI, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TH, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.
- (84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

**Declaration under Rule 4.17:**  
 — of inventorship (Rule 4.17(iv)) for US only

**Published:**  
 — with international search report

[Continued on next page]

(54) Title: PROCESS OF SECURITY OF A UNIT ELECTRONIC UNIT WITH CRYPTOPROCESSOR



(57) Abstract: The invention concerns a process for securing an electronic device incorporating a hardware component capable of autonomous implementation of calculation process  $f$  using one key  $K$ . the process involves calculating at least two new keys  $K^j$  such that at least one of said new keys is identical to key  $K$ , and one of said new keys is different from key  $K$ , and executing said calculation process  $f$  successively with each of said calculated keys  $K^j$ , using said hardware component.

WO 2004/081769 A1





— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

*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.*

## PROCESS OF SECURITY OF A UNIT ELECTRONIC WITH CRYPTOPROCESSOR

The invention concerns a process for securing an electronic device incorporating a hardware component such as a cryptoprocessor, for the purpose of autonomous implementation of a cryptographic algorithm using a secret quantity such as a secret key. In more precise terms, the process is designed to secure said cryptoprocessor against a certain type of physical attacks referred to as Differential Power Analysis (first order electronic attacks or higher) which seek to obtain information concerning the secret key by studying the power consumption of the electronic device during execution of calculations.

15

**TECHNICAL DOMAIN**

Certain components incorporate a hardware DES algorithm. The DES algorithm has the advantage of being extremely fast – of the order of 20 microseconds – and can apparently withstand SPA and DFA type attacks. Unfortunately, it cannot withstand a first order DPA attack. Indeed, with a reasonable number of samples – of the order of 10,000 – it is possible to extract the key. Faced with this vulnerability, it can be necessary to reprogram a secure software DES in full.

25

One purpose of this invention is to propose a process and system for securing components incorporating cryptoprocessors or equivalent devices, in particular against DPA type attacks.

30

The cryptographic algorithms considered here use a secret key to calculate output information according to input information. This can involve an encryption, decryption, signature or signature verification, authentication or non-repudiation operation. The

**CONFIRMATION COPY**

algorithms are constructed in such a way that an attacker with knowledge of the inputs and outputs, cannot in practice deduce any information concerning the secret key itself. Numerous applications base their security on secret key cryptographic algorithms such as the DES, or the more recent AES algorithm, which has now taken its place as the world-wide encryption standard (see John Daemen, Vincent Rijmen; AES proposal; Rijndael: <http://csrc.nist.gov/encryption/aes/rijndael/Rijndael.pdf>).

We are interested in a broader class than that traditionally designated by the expression *secret key algorithm* or *symmetrical algorithm*. In particular, all that is described in this patent application also applies to the so-called public key or asymmetrical algorithms, which in fact incorporate two keys, one public and the other private and not disclosed, the latter being the target for the attacks described below.

The Power Analysis type attacks described by Paul Kocher and Cryptography Research (see document "Introduction to Differential Power Analysis and Related Attacks" by Paul Kocher, Joshua Jaffe and Benjamin Jun, Cryptography Research, 870 Market St., Suite 1008, San Francisco, CA 94102, HTML version of the document accessible at URL address: <http://www.cryptography.com/dpa/technical/index.html>, mentioned in this application for reference purposes) are based on the observation that, in reality, the attacker can acquire information other than simple input and output data, on execution of calculations, such as the power consumption of the microcontroller or the electromagnetic radiation emitted by the circuit, for example. This information, which depends on secret quantities such as the key, leaks from the card.

Differential Power Analysis, abbreviated to DPA, is an attack which makes it possible to obtain information concerning the secret

key contained in the electronic device, by making a statistical analysis of records of power consumption for a large number of calculations with the same key.

We can consider, as a non-exhaustive example, the case of the  
5 DES (Data Encryption Standard) algorithm, a description of which  
can be found in any of the following documents:

FIPS PUB 46-2, Data Encryption Standard, 1994;

FIPS PUB 74, Guidelines for Implementing and Using the NBS Data  
Encryption Standard, 1981;

10 ANSI X3.92, American National Standard, Data Encryption  
Algorithm, 1981;

ISO/IEC 8731:1987, Banking - Approved Algorithms for Message  
Authentication - Part 1: Data Encryption Algorithm (DEA).

Or in the following work:

15 Bruce Schneier, Applied Cryptography, 2nd edition, John Wiley &  
Sons, 1996, page 270.

The above-mentioned documents are indicated in this application for  
reference purposes.

The DES algorithm is executed in 16 steps referred to as  
20 rounds (see Figure 1a). In each of these 16 rounds, conversion F is  
executed on 32 bits. This conversion F uses eight 6-bit to 4-bit non-  
linear conversions, each coded in a table referred to as an S-box (see  
Figure 1b), where the S-boxes are noted S1, S2, ..., S8.

A DPA attack on the DES algorithm can be implemented as  
25 follows:

1st step: Consumption is measured on the first round for 1,000 DES  
calculations. The input values for these 1,000 calculations are noted  
E[1], ..., E[1000]. The 1,000 curves corresponding to power  
consumption measured for these calculations are noted C[1], ...,  
30 C[1,000]. Mean curve CM is also calculated for the 1,000  
consumption curves.

2nd step: We consider the first output bit from the first S-box on the first round, for example. The value of this bit is noted  $b$ . It is easy to see that  $b$  only depends on 6 bits of the secret key. The attacker makes an assumption concerning the 6 bits concerned. The attacker  
5 calculates the theoretical values expected for  $b$  from these 6 bits and the  $E[i]$ . This makes it possible to separate the 1,000 inputs  $E[1], \dots, E[1,000]$  into two categories: those which give  $b=0$ , and those which give  $b=1$ .

3rd step: Mean value  $CM'$  is then calculated for the curves  
10 corresponding to the first category inputs, namely those for which  $b=0$ . If  $CM$  and  $CM'$  show a marked difference, it is considered that the values adopted for the 6 bits of the key were correct. If  $CM$  and  $CM'$  do not show a marked difference in the statistical sense, namely no difference substantially greater than the typical variance for the  
15 noise measured, the 2nd step is repeated with a different selection for the 6 bits.

4th step: Steps 2 and 3 are repeated with a target bit  $b$  from the second S-box, and then from the third S-box, and so on up to the eighth S-box. Forty-eight bits of the secret key are finally obtained in  
20 this way.

5th step: The 8 remaining bits can be found by exhaustive search.

This attack requires no knowledge concerning the individual power consumption of each instruction, nor the position in time of each of these instructions. It applies in the same way if we assume  
25 that the attacker knows the outputs of the algorithm and corresponding consumption curves. It is based solely on the following fundamental assumption:

Fundamental assumption: An intermediate variable exists, appearing during the course of calculation of the algorithm, such that  
30 knowledge of a few key bits, in practice less than 32 bits, is sufficient to decide whether two inputs, respectively two outputs, give the same

value for this variable or not.

All algorithms using the S-box principle, such as the DES algorithm, are potentially vulnerable to DPA attack, as the customary methods of implementation generally lie within the framework of the assumption mentioned above.

So-called High-Order Differential Power Analysis attacks, abbreviated to HO-DPA, correspond to generalisation of the DPA type attack described above. They can use a number of different information sources apart from consumption, and can involve measurement of electromagnetic radiation, temperature, etc., and employ more sophisticated statistical processing than the simple notion of average, with less elementary intermediate variables (generalising bit  $b$  defined above). Nevertheless, they are based on precisely the same fundamental assumption as the DPA attack.

15

**SUMMARY OF THE INVENTION**

The invention concerns a process for securing an electronic device incorporating a hardware component capable of autonomous implementation of a calculation process using key  $K$ , characterised by the fact that it involves calculating at least two new keys  $K^i$  such that for at least one given  $i=j$ ,  $K^j=K$  and for at least one  $i=t$ ,  $K^t \neq K$ , and executing said calculation process with each of said calculated keys  $K^i$  in succession, using said hardware component.

According to one particular form of implementation, the process involves calculating  $l=\alpha$   $m$  new keys  $K^1, \dots, K^l$ , so that for a given  $j$  ( $0 < j < n+1$ ), sub-keys  $K^i_j$  ( $0 < i < l+1$ ) take all the possible values, including the value of sub-key  $K_j$ , and executing hardware cryptographic function  $f$  with these  $l$  new keys  $K^1, \dots, K^l$ , in a random manner.

The invention also concerns an electronic device and a smart card for example, and a program for implementation of the process.

**BRIEF DESCRIPTION OF THE DRAWINGS**

Other purposes, advantages and characteristics of the invention will emerge from the following description of implementation of the process according to the invention, and of a method of execution of an electronic device adapted for this implementation, given for non-exhaustive example purposes referring to the appended drawings where:

- Figure 1 shows an electronic device according to the invention in schematic form;

- Figure 2 shows a hardware component of said device according to Figure 1 in schematic form;
- Figure 3 shows the process according to the invention in schematic form.

5

### IMPLEMENTATION OF THE INVENTION

The process according to the invention is designed to secure an electronic device, for example an on-board system such as a smart card implementing a cryptographic calculation process which uses a secret key. The electronic device incorporates means to process information, such as a processor, and means to store information such as a memory.

As a non-exhaustive example, the electronic device described below corresponds to an on-board system incorporating electronic module 1 as shown in Figure 1. Modules of this type usually take the form of a monolithic integrated electronic microcircuit or chip, which, once protected physically by any known means, can be mounted on a portable object such as a smart card, microcircuit card or other which can be used in various domains, for example.

Microprocessor electronic module 1 comprises CPU microprocessor 3, connected bidirectionally via internal bus 5 to a non-volatile memory 7 of the ROM, EEPROM, Flash, FeRam or other type containing an executable program, RAM memory 11, I/O device 13 for communication with the exterior, and cryptoprocessor calculation unit 15 (CRYPTO P), this component being capable of autonomous cryptographic calculation, such as calculation of a DES algorithm, for example. As shown in Figure 2, cryptoprocessor 15 of said module 1 executes calculation process f using secret key K, stored in a secret zone of a memory, for example of the EEPROM type, on a message M.



We will firstly consider the solution in its general form. As shown in Figure 3, the objective is to calculate result  $E(M,K)$  of cryptographic function  $E$  on message  $M$ , using key  $K$ . For this purpose, we have function  $f$ , which, in its capacity as a black box, executes the same calculation as  $E$  but cannot withstand DPA attack in particular. We also consider that key  $K$  acts in regard to the algorithm in the form of  $n$  small sub-keys  $m_b$  (taking  $m_b < 10$  bits, or  $m = 2^{m_b}$  possible values for each sub-key), which will then be noted  $K_1, K_2, \dots, K_n$ , and which will be susceptible to DPA attack in particular. The sub-keys are of the same size in the form of implementation described below. The invention also applies for sub-keys of a different size.

The invention involves associating external software module 17 with the cryptoprocessor, to secure the cryptographic function implemented by said cryptoprocessor 15.

As shown in Figure 3, the invention involves calculating  $I = \alpha m$  new keys  $K^1, \dots, K^I$ , so that for a given  $j$  ( $0 < j < n+1$ ), each sub-key  $K^i_j$  ( $0 < i < I+1$ ) takes all the possible values, and according to a special form of implementation  $\alpha$  times, including the value of sub-key  $K_j$ , and executing hardware cryptographic function  $f$  with these  $I$  new keys  $K^1, \dots, K^I$  in a random manner.

In other words, the idea is to execute  $I = \alpha m$  successive calculations with keys  $K^i$ ,  $0 \leq i < I$ , such that:

there exists  $i$  such that  $K^i = K$ .

For all the  $j$ , we have  $\{ K^i_j, 0 \leq i < I \} = \{ 0, 1, \dots, m-1 \}$ , with each sub-key appearing exactly  $\alpha$  times.

This means in fact that we will execute a number of successive calculations with different keys (including the true key), in such a way that each possible sub-key appears the same number of times.

The calculations will also be executed in a random order. Consequently, the attacker has no chance of identifying the correct sub-key by DPA attack, as this sub-key appears neither more nor less frequently than any other.

5           We will now see how this countermeasure (noted CM in the following paragraphs) applies to different algorithms.

#### Simple application to the DES algorithm

#### 10   Notations

          We will adopt the following notations for the DES algorithm:

PC1 represents the initial permutation of the key, reducing the key from 64 to 56 bits.

15   IPC1 represents the inverse of PC1 (56 bits to 64), where the 8 missing bits are completed (parity bits are frequently used).

PC2 represents the combination of compressive permutation (56 bits to 48 bits) and shift of the key to the first round.

IPC2 represents the inverse of PC2 (48 to 56 bits), where the 8  
20   undetermined bits ( $8=56-48$ ) are selected arbitrarily (for example randomly).

The permutation from 48 bits to 64 bits (combination of IPC2 and IPC1) is noted PP.

25           We see that PP makes it possible, starting from key K48 with 48 bits, used in the first round of the DES algorithm, to reach global key  $K64 = PP(K48)$  having the following property: using K64 as the key for a DES calculation, we obtain K48 as the first sub-key in the first round.

30

We will now see how we can apply our countermeasure in concrete terms.

1.1 Initial implementation of the CM

5

In the case of the DES algorithm, the sub-keys are used in the form of n=8 sub-keys of mb=6 bits each, giving m=64 possibilities. We shall then execute 64 successive calculations ( $\alpha = 1$ ) with the following derivative keys:

10

$K_{00} = K \oplus PP(000000 | 000000 | \dots | 000000 | 000000)$   
 $K_{01} = K \oplus PP(000001 | 000001 | \dots | 000001 | 000001)$   
 $K_{02} = K \oplus PP(000010 | 000010 | \dots | 000010 | 000010)$   
 $K_{03} = K \oplus PP(000011 | 000011 | \dots | 000011 | 000011)$

15

.  
.  
.  
 $K_{61} = K \oplus PP(111101 | 111101 | \dots | 111101 | 111101)$   
 $K_{62} = K \oplus PP(111110 | 111110 | \dots | 111110 | 111110)$   
 $K_{63} = K \oplus PP(111111 | 111111 | \dots | 111111 | 111111)$

20

It is thus easy to see that for each of the eight sub-keys used in the first round, the 64 possible values are represented equally, and that true key K00 is present in the list. It is then merely necessary to execute 64 DES calculations with the 64 derivative keys in a random order, and select the final result as being that where the correct key has been used.

25

30

This can be done in the following way. Sixteen memory bytes are allocated to store the result. An additional byte is also allocated for each  $K_i$  (initialised in this case at 0 or 8), which will indicate the byte from which the result is stored in memory. Thus, this byte will take the value 8 for all keys except K00 for which it will take the value 0. This makes it possible to use a relatively generic code, which could resemble the next pseudo-code C, considering that we have one

35

function executing a memory copy, one which calculates the PP(i | ... | i) and one which randomizes the 64 keys.

```

5   void
    DES_encrypt_DPA( unsigned char in[8],
                    unsigned char cle[8],
                    unsigned char out[8] )
    {
10  int i;
    unsigned char M1[8], M2[16], K[64][9];

    memcpy(K[0],cle,8);
    K[0][8] = 0;
15  for(i=1; i<64; i++)
    {
    memcpy(K[i], cle XOR PP(i | ... | i), 8);
    K[i][8] = 8;
20  }

    randomize_0_63(K);

    for(i=0; i<64; i++)
25  {
    memcpy(M1, in, 8);
    DES_encrypt_non_DPA(M1,K[i]);

    for(j=0;j<8;j++)
30  {
    M2[K[i][8] + j] = M1[j];
    }
    }

35  memcpy(out, M2, 8);
    }

```

## 40 1.2 General security considerations

From the DPA point of view, it is easy to see that any attacker, unable to distinguish for each of the 64 executions of the DES algorithm whether the true key is concerned or not, cannot attack the algorithm with a conventional DPA. However, it must be remembered  
45 that programming of the method requires a very strict approach, as any analysis making it possible to distinguish – even rarely – the

correct key destroys the CM completely! Attention must therefore be paid to the following critical points:

- 5           - Randomization: this step shifts the true key to location  $0 \leq i < 64$  which must be unknown to the exterior.
- Result copy (loop to j): here again, the two values (0 or 8), which would enable the attacker, if revealed, to know which DES algorithm uses the true key, are involved.

### 10           3.4 CM extensions and various aspects

- 15           - If we take a closer look at function PP, it is easy to see that it is not necessary to use the same value for the eight sub-keys, as was done previously, to mask the key. Taking sub-key i, it is merely necessary for the 64 possible values to appear. It is not necessary for the order of the 64 values to be the same for a given sub-key as for another sub-key! The only requirement is that the value 0 of the sub-key (for which the true sub-key is used) appears at the same time
- 20           for the eight sub-keys, so that one of the 64 calculations gives the correct result. We can thus imagine a derivation of the following type:

25            $K_{00} = K \oplus PP( 000000 | 000000 | \dots | 000000 | 000000 )$   
 $K_{01} = K \oplus PP( 011000 | 001101 | \dots | 001001 | 111100 )$   
 $K_{02} = K \oplus PP( 010101 | 001111 | \dots | 001011 | 010000 )$   
 $K_{03} = K \oplus PP( 110011 | 100010 | \dots | 000011 | 010010 )$

30            $K_{51} = K \oplus PP( 101011 | 011100 | \dots | 110001 | 101000 )$   
 $K_{52} = K \oplus PP( 100111 | 101010 | \dots | 000110 | 010111 )$   
 $K_{53} = K \oplus PP( 001110 | 010111 | \dots | 011100 | 110001 )$

- 35           This merely requires a function which executes a random permutation of the values [1,63].

It should be noted that the fact that the mask ( 000000 | ... | 000000 ) always appears in the initial position does not represent a problem, as the derivative keys are then permuted randomly before being used. If we consider that we have a function PP2(i,val) which  
 5 replaces the 6 bits of value val in the correct position for it to correspond to sub-key i, we then obtain the following pseudo-code C:

```

10 void
    DES_encrypt_DPA(unsigned char in[8],
                   unsigned char cle[8],
                   unsigned char out[8] )
    {
15     int i,j;
        unsigned char M1[8], M2[16], K[64][9];

        memcpy(K[0],cle,8);
        K[0][8] = 0;
20     for(i=0;i<64;i++)
        {
            memcpy(K[i],cle,8);
        }
25     for(i=0; i<8; i++)
        {
            unsigned char Perm63[63];

            randomize_1_63(Perm63);
            for(j=1; j<64; j++)
            {
30                K[j] = K[j] XOR PP2(i,Perm[j]);
            }
        }
35     }

    randomize_0_63(K);

    for(i=0; i<64; i++)
40     {
        memcpy(M1, in, 8);
        DES_encrypt_non_DPA(M1,K[i]);

        for(j=0;j<8;j++)
45         {
            M2[K[i][8] + j] = M1[j];
        }
    }
  
```

```
    memcpy(out, M2, 8);  
}
```

5

- Randomization of the 64 derivative keys can be performed using the following conventional method (cf. Crypto'2002 or Akkar/Goubin article on HODPA attacks on the DES algorithm), which involves scanning the keys from 0 to 63 with index *i*, and exchanging the key with index *i* with a key with an index selected randomly between 0 and 63:

10

```
void  
15 randomize(unsigned char table[64])  
{  
    int i, i_temp;  
    unsigned char temp;  
20    for(i=0; i<64; i++)  
    {  
        table[i] = i;  
    }  
25    for(i=0; i<64; i++)  
    {  
        i_temp = random() % 64;  
        temp = table[i];  
        table[i] = table[i_temp];  
30        table[i_temp] = temp;  
    }  
}
```

### 3.5 Other DES rounds

35

We have seen how to protect the first DES round against DPA attack. Where the DES is more vulnerable on the 16th round in the protocol used, a similar method can naturally be envisaged. Only function PP will change, and correspond to the key-scheduling for the 16th round! It is then possible to use 64 key masks which protect both the first and last rounds. The following 64 key mask keys possess this property:

40

```

0000000000000000 8444054405410000 410900B100033003
    C54D05F505423003
0093420342004141 84D7474747414141 419A42B242037142
    C5DE47F647427142
5 0021000000950C9C 8465054405D40C9C 412800E100963C9F
    C56C05F505D73C9F
00B2420342954DDD 84F6474747D44DDD 41BB42B242967DDE
    C5FF47F647D77DDE
10 2200300918288100 A644354D1D698100 630930B8182BB103
    E74D35FC1D6AB103
2293720A5A28C041 A6D7774E5F69C041 639A72BB5A2BF042
    E7DE77FF5F6AF042
2221300918BD8D9C A665354D1DFC8D9C 632830B818BEBD9F
    E76C35FC1DFFBD9F
15 22B2720A5ABDCCDD A6F6774E5FFCCDD 63BB72BB5ABEFCDE
    E7FF77FF5FFFCDDE
18008800A0000321 9C448D44A5410321 590988B1A0033322
    DD4D8DF5A5423322
1893CA03E2004260 9CD7CF47E7414260 599ACAB2E2037263
    DDDECF6E7427263
20 18218800A0950FBD 9C658D44A5D40FBD 592888B1A0963FBE
    DD6C8DF5A5D73FBE
18B2CA03E2954EFC 9CF6CF47E7D44EFC 59BBCAB2E2967EFF
    DDFFCFF6E7D77EFF
25 3A00B809B8288221 BE44BD4DBD698221 7B09B8B8B82BB222
    FF4DBDFCBD6AB222
3A93FA0AFA28C360 BED7FF4EFF69C360 7B9AFABBFA2BF363
    FFDEFFFFFFF6AF363
3A21B809B8BD8EBD BE65BD4DBDFC8EBD 7B28B8B8B8BEBEBE
    FF6CBDFCBDFFBEBE
30 3AB2FA0AFABDCFFC BEF6FF4EFFFCFFC 7BBBFABBFABEFFFF
    FFFFFFFF

```

Obviously, this countermeasure (or at least the critical parts)  
 must be implemented in the assembler mode, so as to avoid  
 introducing vulnerability due to unfamiliarity with the methods used  
 by the compiler.

2. Application to the AES algorithm

Obviously, this method can apply in a similar way to the AES  
 algorithm. This is even simpler to explain, as the first sub-key used –  
 which is frequently the target – comprises the key with no other  
 conversion! Another practical difference stems from the fact that the  
 key occurs 8 bits by 8 bits. Thus, in the case of an AES algorithm  
 with key and 128-bit message, we obtain key derivation and a



16

pseudo-code C as follows:

```

5   K00 = K ⊕ ( 00000000 | 00000000 | ... | 00000000 | 00000000 )
   K01 = K ⊕ ( 00000001 | 00000001 | ... | 00000001 | 00000001 )
   K02 = K ⊕ ( 00000010 | 00000010 | ... | 00000010 | 00000010 )
   K03 = K ⊕ ( 00000011 | 00000011 | ... | 00000011 | 00000011 )
   .
10  .
   K61 = K ⊕ ( 11111101 | 11111101 | ... | 11111101 | 11111101 )
   K62 = K ⊕ ( 11111110 | 11111110 | ... | 11111110 | 11111110 )
   K63 = K ⊕ ( 11111111 | 11111111 | ... | 11111111 | 11111111 )

15

   void
   AES_encrypt_DPA( unsigned char in[16],
20                   unsigned char cle[16],
                   unsigned char out[16] )
   {
       int i;
       unsigned char M1[16], M2[32], K[256][17];
25
       memcpy(K[0], cle, 16);
       K[0][16] = 0;

       for(i=1; i<256; i++)
30     {
           memcpy(K[i], cle XOR (i | ... | i), 16);
           K[i][8] = 16;
       }

35     randomize_0_255(K);

       for(i=0; i<256; i++)
       {
           memcpy(M1, in, 16);
40           AES_encrypt_non_DPA(M1, K[i]);

           for(j=0; j<16; j++)
           {
45               M2[K[i][16] + j] = M1[j];
           }
       }

       memcpy(out, M2, 16);
50     }

```

The only real difference is that key-scheduling for the AES algorithm is not linear, in contrast to the DES, except for the first

sub-key. Thus, if we wish to protect the last round by this method, a method similar to the DES cannot be considered. It is then necessary to store the set of 256 keys specific to a given key, instead of the key derivation plan.

5

### 3. Conclusion

We thus see that it is possible, by execution of 64 DES (or 256  
10 AES) algorithms and a number of ancillary calculations, to protect a cryptographic algorithm (DES or AES, for example) against DPA attack by means of a rapid although unprotected brick. Sixty-four DES or 256 AES may appear long, nevertheless in practice these hardware operations take a practically negligible amount of time.

15

**CLAIMS**

1. Process for securing an electronic device incorporating a hardware component capable of autonomous implementation of calculation process  $f$  using key  $K$ , characterised by the fact that it  
5 involves calculating at least two new keys  $K^i$  such that at least one of said new keys is identical to key  $K$ , and at least one of said new keys is different from key  $K$ , and executing said calculation process  $f$  successively with each of said calculated keys  $K^i$  using said hardware  
10 component.

2. Process according to claim 1, characterised in that it involves executing said calculation process with said keys  $K^i$  in a random order.

3. Process according to claim 1 or 2, characterised in that key  
15  $K$  is sub-divided into sub-keys  $K_1, \dots, K_n$ , and that there exists at least one  $i$  such that key  $K^i$  is different from  $K$  for at least one sub-key  $K^i_j$ .

4. Process according to one of claims 1 to 3, characterised in that key  $K$  is sub-divided into sub-keys  $K_1, \dots, K_n$ , and that the  
20 procedure involves calculating  $I=\alpha$   $m$  new keys  $K^1, \dots, K^m$ , where  $m$  represents the number of possible values for one of sub-keys  $K^i_j$  of  $K^i$ , in such a way that for a given  $j$  ( $0 < j < n+1$ ), sub-keys  $K^i_j$  ( $0 < i < l+1$ ) take all the possible values, including the value of sub-key  $K_j$  of  $K$ .

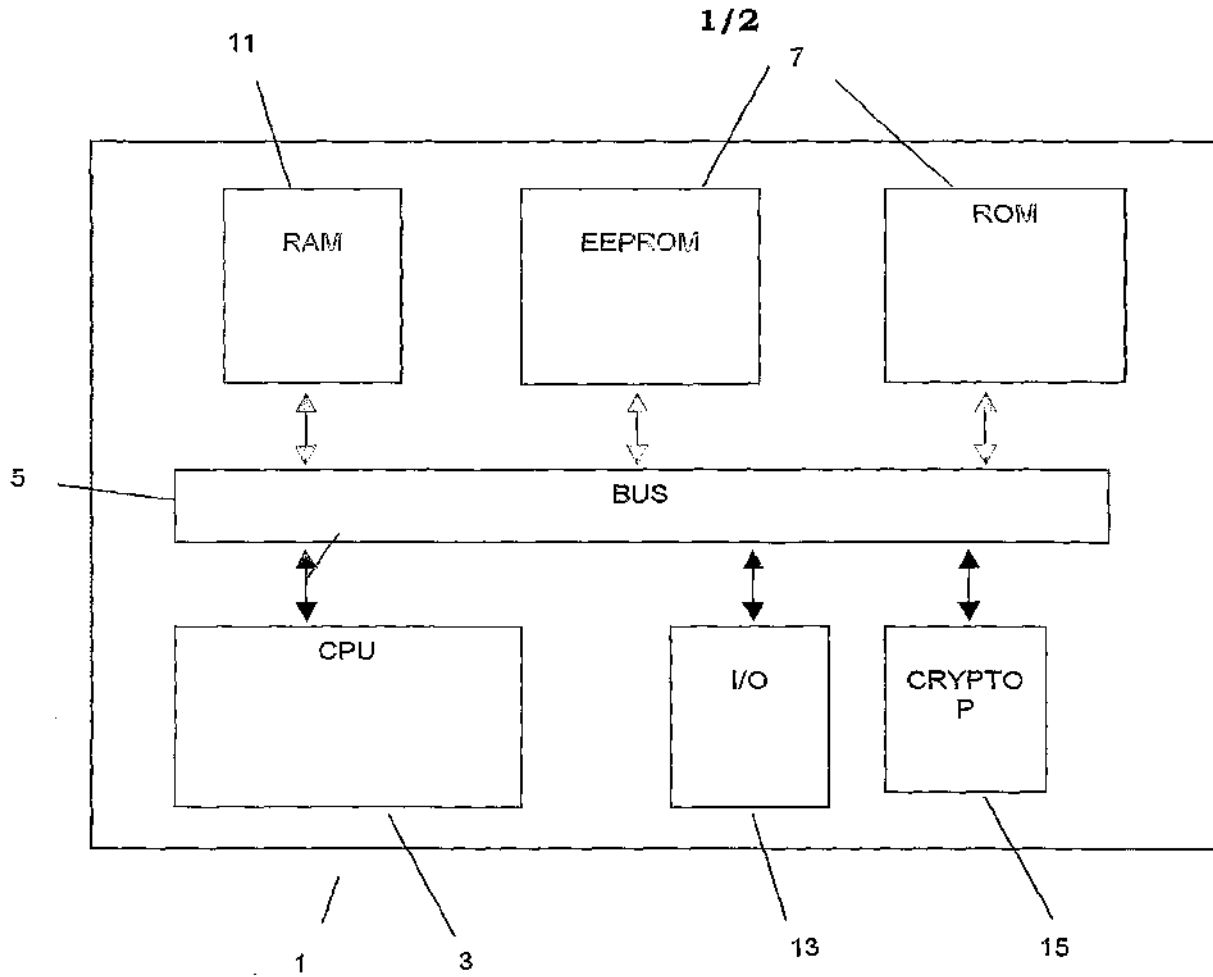
5. Process according to claim 4, characterised in that sub-keys  
25  $K^i_j$  ( $0 < i < l+1$ ) take all the possible values  $\alpha$  times.

6. Electronic device incorporating means to store a calculation process, means to execute said process and a hardware component capable of autonomous implementation of a calculation process using

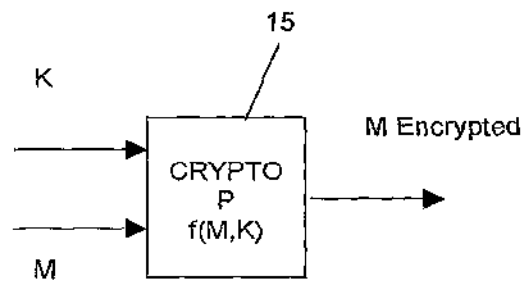
key K, characterised in that it incorporates a software module associated with the hardware component, capable of calculating at least two new keys  $K^i$ , such that at least one of new said keys is identical to key K, and one of said new keys is different from key K, and in that the software module is associated with the hardware component in such a way as to be able to transmit in succession to said hardware component, the new keys calculated to implement said calculation process with each of said new keys  $K^i$ .

7. Electronic device according to claim 6, characterised in that said software module transmits in succession the new keys calculated in a random order.

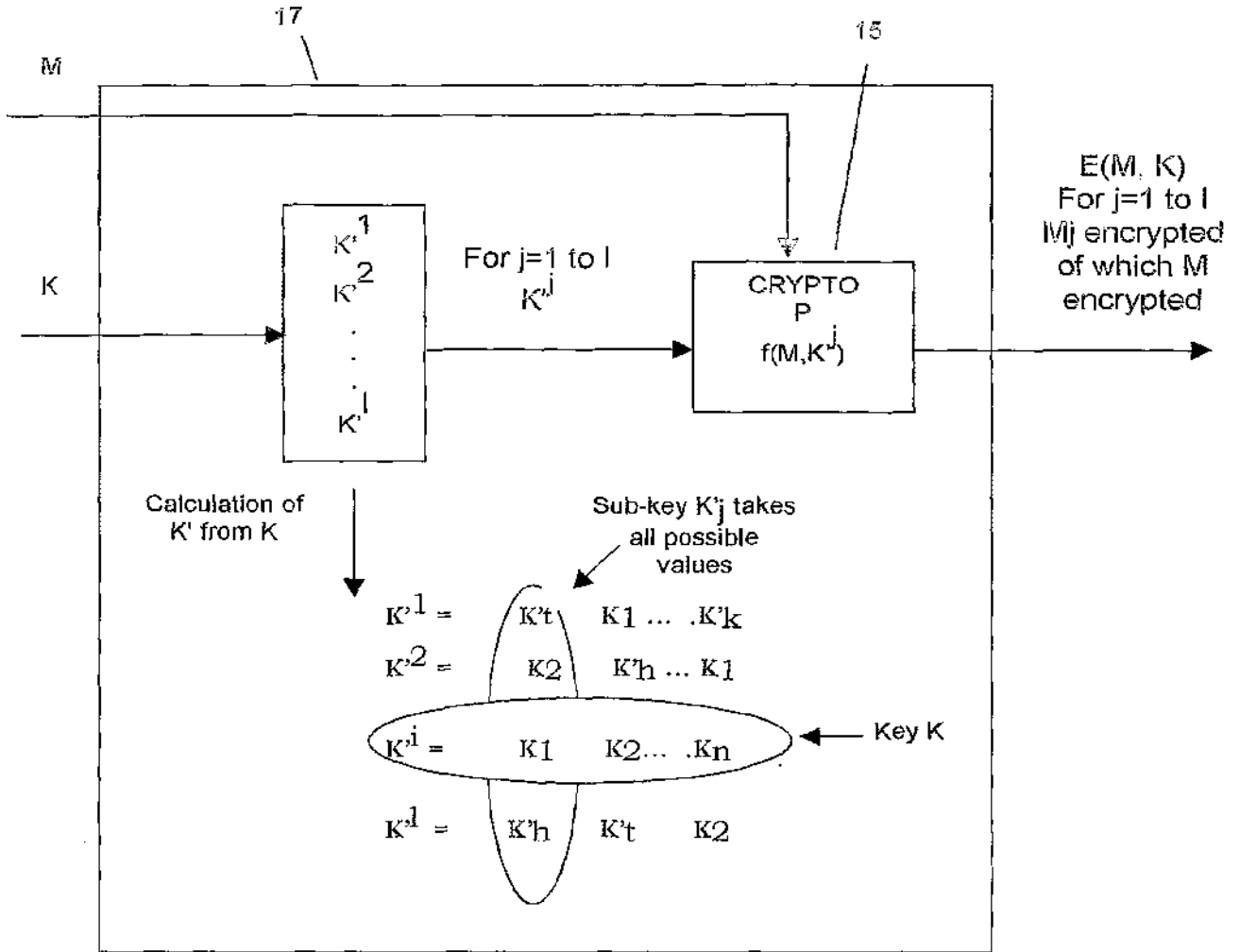
8. Computer program incorporating program code instructions for execution of the steps of the process according to one of claims 1 to 5, when said program is executed in an electronic device.



**FIG. 1**



**FIG. 2**



**FIG. 3**

# INTERNATIONAL SEARCH REPORT

International Application No  
PCT/IB2004/000738

**A. CLASSIFICATION OF SUBJECT MATTER**  
IPC 7 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 7 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

EPO-Internal, WPI Data

**C. DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 01/31422 A (VON WILlich MANFRED) 3 May 2001 (2001-05-03) page 3, line 11 - line 37 page 5, line 26 - page 6, line 37 page 8, line 27 - page 9, line 20 page 11, line 17 - line 29 page 12, line 7 - line 14 claims 1,3 figures 8,9 <div style="text-align: center; margin-top: 20px;">----- -/--</div>	1-8

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.
- \*Z\* document member of the same patent family

Date of the actual completion of the international search

20 July 2004

Date of mailing of the international search report

05/08/2004

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

Bichler, M

# INTERNATIONAL SEARCH REPORT

International Application No  
PCT/IB2004/000738

**C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT**

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	<p>CHARI S ET AL: "TOWARDS SOUND APPROACHES TO COUNTERACT POWER-ANALYSIS ATTACKS" ADVANCES IN CRYPTOLOGY. CRYPTO '99. 19TH ANNUAL INTERNATIONAL CRYPTOLOGY CONFERENCE. SANTA BARBARA, CA, AUG. 15 - 19, 1999. PROCEEDINGS, LECTURE NOTES IN COMPUTER SCIENCE;VOL. 1666, BERLIN: SPRINGER, DE, 1999, pages 398-412, XP000911819 ISBN: 3-540-66347-9 abstract page 402 - page 404</p>	1-8
A	<p>EP 1 109 350 A (SAGEM) 20 June 2001 (2001-06-20) page 3, paragraph 24 - page 4, paragraph 30</p>	1-8



# INTERNATIONAL SEARCH REPORT

Information on patent family members

In:      onal Application No  
PCT/IB2004/000738

Patent document cited in search report		Publication date		Patent family member(s)	Publication date
WO 0131422	A	03-05-2001	AU	773982 B2	10-06-2004
			AU	2301401 A	08-05-2001
			CA	2388971 A1	03-05-2001
			CN	1413398 T	23-04-2003
			EA	3874 B1	30-10-2003
			EP	1226681 A2	31-07-2002
			JP	2003513490 T	08-04-2003
			WO	0131422 A2	03-05-2001
			ZA	200202798 A	10-07-2003
			<hr style="border-top: 1px dashed black;"/>		
EP 1109350	A	20-06-2001	FR	2802741 A1	22-06-2001
			EP	1109350 A1	20-06-2001
<hr style="border-top: 1px dashed black;"/>					

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	1032194
<b>Application Number:</b>	10990296
<b>Confirmation Number:</b>	2050
<b>Title of Invention:</b>	Multi-interface compact personal token apparatus and methods of use
<b>First Named Inventor:</b>	Dennis J. Ryan
<b>Customer Number:</b>	37053
<b>Filer:</b>	Dwight A. Stauffer
<b>Filer Authorized By:</b>	
<b>Attorney Docket Number:</b>	Ryan C-4
<b>Receipt Date:</b>	26-APR-2006
<b>Filing Date:</b>	16-NOV-2004
<b>Time Stamp:</b>	19:57:02
<b>Application Type:</b>	Utility
<b>International Application Number:</b>	

### Payment information:

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

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part	Pages
1	Information Disclosure Statement (IDS) Filed	Ryan C-4 IDS as re-filed 4-26-06.pdf	330312	no	3

<b>Warnings:</b>					
<b>Information:</b>					
This is not an USPTO supplied IDS fillable form					
2	Foreign Reference	DE19631050.pdf	185970	no	4
<b>Warnings:</b>					
<b>Information:</b>					
3	Foreign Reference	HK1063994.pdf	885012	no	14
<b>Warnings:</b>					
<b>Information:</b>					
4	Foreign Reference	HK1063995.pdf	518447	no	11
<b>Warnings:</b>					
<b>Information:</b>					
5	Foreign Reference	JP2004246720.pdf	907350	no	23
<b>Warnings:</b>					
<b>Information:</b>					
6	Foreign Reference	WO99-052051.pdf	951330	no	26
<b>Warnings:</b>					
<b>Information:</b>					
7	Foreign Reference	WO99-038062.pdf	604741	no	16
<b>Warnings:</b>					
<b>Information:</b>					
8	Foreign Reference	WO00-036252.pdf	965881	no	27
<b>Warnings:</b>					
<b>Information:</b>					
9	Foreign Reference	WO00-042491.pdf	2287491	no	57
<b>Warnings:</b>					
<b>Information:</b>					

10	Foreign Reference	WO00-065180.pdf	540410	no	14
<b>Warnings:</b>					
<b>Information:</b>					
11	Foreign Reference	WO00-075755.pdf	1004753	no	40
<b>Warnings:</b>					
<b>Information:</b>					
12	Foreign Reference	WO01-014179.pdf	2071078	no	56
<b>Warnings:</b>					
<b>Information:</b>					
13	Foreign Reference	WO01-038673.pdf	1396174	no	38
<b>Warnings:</b>					
<b>Information:</b>					
14	Foreign Reference	WO01-039102.pdf	784012	no	14
<b>Warnings:</b>					
<b>Information:</b>					
15	Foreign Reference	WO01-048339.pdf	1049894	no	27
<b>Warnings:</b>					
<b>Information:</b>					
16	Foreign Reference	WO01-048342.pdf	1098879	no	30
<b>Warnings:</b>					
<b>Information:</b>					
17	Foreign Reference	WO01-061692.pdf	531955	no	18
<b>Warnings:</b>					
<b>Information:</b>					
18	Foreign Reference	WO01-088693.pdf	862354	no	22
<b>Warnings:</b>					
<b>Information:</b>					

19	Foreign Reference	WO01-096990.pdf	1414740	no	33
<b>Warnings:</b>					
<b>Information:</b>					
20	Foreign Reference	WO03-014887.pdf	908231	no	21
<b>Warnings:</b>					
<b>Information:</b>					
21	Foreign Reference	WO03-034189.pdf	820620	no	24
<b>Warnings:</b>					
<b>Information:</b>					
22	Foreign Reference	WO04-002058.pdf	1049219	no	28
<b>Warnings:</b>					
<b>Information:</b>					
23	Foreign Reference	WO04-081706.pdf	1042944	no	22
<b>Warnings:</b>					
<b>Information:</b>					
24	Foreign Reference	WO04-081769.pdf	1009649	no	26
<b>Warnings:</b>					
<b>Information:</b>					
25	NPL Documents	NPL-1_ACR38CT.pdf	231033	no	4
<b>Warnings:</b>					
<b>Information:</b>					
26	NPL Documents	NPL-2_ACR38DT.pdf	467142	no	4
<b>Warnings:</b>					
<b>Information:</b>					
27	NPL Documents	NPL-4_DS9490R-DS9490B.pdf	212025	no	5
<b>Warnings:</b>					
<b>Information:</b>					

28	NPL Documents	NPL-5_Hara-ee-times-FeRAM.pdf	28457	no	1
<b>Warnings:</b>					
<b>Information:</b>					
29	NPL Documents	NPL-7_Oti-6828.pdf	380125	no	7
<b>Warnings:</b>					
<b>Information:</b>					
30	NPL Documents	NPL-9_Panasonic-contactless-JCNN htm.pdf	36896	no	3
<b>Warnings:</b>					
<b>Information:</b>					
31	NPL Documents	NPL-11_Philips-Delivering-SmartMX.tif.pdf	34270	no	1
<b>Warnings:</b>					
<b>Information:</b>					
32	NPL Documents	NPL-12_Balaban-SIMS_v_Flash-Cards.tif.pdf	451360	no	5
<b>Warnings:</b>					
<b>Information:</b>					
33	NPL Documents	NPL-13_SmartMX-P5GT072.pdf	539555	no	12
<b>Warnings:</b>					
<b>Information:</b>					
34	NPL Documents	NPL-15_Panasonic-Smart-SD-Card.jpg.pdf	41613	no	1
<b>Warnings:</b>					
<b>Information:</b>					
35	NPL Documents	NPL-3_Dallas-DS1490F.pdf	139760	no	3
<b>Warnings:</b>					
<b>Information:</b>					
36	NPL Documents	NPL-6__JP-Matsushita-Mercury-New.pdf	44980	no	2
<b>Warnings:</b>					
<b>Information:</b>					

37	NPL Documents	NPL-8__Panasonic-palm-info-cente.pdf	87632	no	3
<b>Warnings:</b>					
<b>Information:</b>					
38	NPL Documents	NPL-10_Rojas-Panasonic-smart-SD.pdf	104731	no	4
<b>Warnings:</b>					
<b>Information:</b>					
39	NPL Documents	NPL-14__Vodafone-Develops htm.pdf	36700	no	2
<b>Warnings:</b>					
<b>Information:</b>					
<b>Total Files Size (in bytes):</b>			26057725		

**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.**

**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 <input type="checkbox"/>		

SMALL ENTITY TYPE

OR OTHER THAN SMALL ENTITY

RATE	FEE
BASIC FEE	395
X\$ 25=	800
X100=	
+180=	
TOTAL	1195

RATE	FEE
BASIC FEE	790
X\$50=	
X200=	
+360=	
TOTAL	

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

11/14/05 **CLAIMS AS AMENDED - PART II**

	(Column 1)	(Column 2)	(Column 3)
AMENDMENT A	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
Total	52	52	
Independent	3	3	
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <input checked="" type="checkbox"/>			

RATE	ADDI-TIONAL FEE
X\$ 25=	
X100=	
+180=	
TOTAL	

RATE	ADDI-TIONAL FEE
X\$50=	
X200=	
+360=	
TOTAL	

	(Column 1)	(Column 2)	(Column 3)
AMENDMENT B	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
Total	58	52	6
Independent	4	3	1
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <input type="checkbox"/>			

RATE	ADDI-TIONAL FEE
X\$ 25=	150 <sup>00</sup>
X100=	100 <sup>00</sup>
+180=	
TOTAL	250 <sup>00</sup>

RATE	ADDI-TIONAL FEE
X\$50=	
X200=	
+360=	
TOTAL	

	(Column 1)	(Column 2)	(Column 3)
AMENDMENT C	CLAIMS REMAINING AFTER AMENDMENT	HIGHEST NUMBER PREVIOUSLY PAID FOR	PRESENT EXTRA
Total			
Independent			
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM <input type="checkbox"/>			

RATE	ADDI-TIONAL FEE
X\$ 25=	
X100=	
+180=	

RATE	ADDI-TIONAL FEE
X\$50=	
X200=	
+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 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      09/14/2006

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

EXAMINER
----------

LE, UYEN CHAU N

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

2876

DATE MAILED: 09/14/2006

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

<b>Office Action Summary</b>	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 25 April 2006.
- 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) 1-33,35-48 and 50-60 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) 1-33,35-48 and 50-60 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/SB/08)  
 Paper No(s)/Mail Date 04/26/2006
- 4)  Interview Summary (PTO-413)  
 Paper No(s)/Mail Date. \_\_\_\_\_
- 5)  Notice of Informal Patent Application
- 6)  Other: \_\_\_\_\_

**DETAILED ACTION**

***Requesting Continued Examination (RCE)***

1. Receipt is acknowledged of the Requesting Continued Examination (RCE) field 04/25/2006.

***Claim Objections***

2. Claims 2, 5, 21, 22, 26, 35, 37, 42, 43, 54-56 and 60 are objected to because of the following informalities:

Re claims 2, 5, 21, 22, 26, 35, 37, 42, 43, 54-56 and 60:  
The additional word "similar" recited in the claims understood as "the like", which renders the claims to indefinite.

Appropriate correction is required.

***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 (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

Art Unit: 2876

States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1, 8, 18-29, 31-33 and 35-40 are rejected under 35 U.S.C. 102(e) as being anticipated by Jiau (US 2003/0236821 A1).

Re claims 1, 8, 18-29, 31-33 and 35-40: 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 802.11 and Bluetooth compatible interface (paragraphs [0047] & [0050]); a flash memory 133 (fig. 3A); wherein: the dual interface chip (processor) inside the personal

Art Unit: 2876

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***

5. 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.

Art Unit: 2876

6. 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).

7. Claims 1-7, 9, 12-17, 21, 41-48 and 50-60 are rejected under 35 U.S.C. 103(a) as being unpatentable over Margalit et al (US 6,748,541) in view of Weng (US 6983888 B2).

Re claims 1-7, 9, 12-17, 21, 41-48 and 50-60: 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;

Art Unit: 2876

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

Art Unit: 2876

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).

Margalit et al is silent with respect to the translation module moves signals from the connection module to a contactless interface.

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 Margalit et al due to the fact that such modification would have been an



Art Unit: 2876

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 vice versa), and therefore an obvious expedient.

8. 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

Art Unit: 2876

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 vice versa), and therefore an obvious expedient.

9. 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

Art Unit: 2876

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***

10. Applicant's arguments with respect to claims 1 and 46 (i.e., with respect to Margalit reference) have been considered but are moot in view of the new ground(s) of rejection.

11. 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 apparatus has USB interface, wireless interface, contactless interface (p. 19, lines 10-16)) 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). In this case, although both former and newly amended claims 1 and 46 have been carefully reviewed and given all possible ways of interpretation, an

Art Unit: 2876

apparatus having all three specific components (e.g., USB interface, wireless interface, contactless interface) cannot be obtained.

12. Applicant's arguments regarding claims 1, 8, 18-29 and 31-40 with respect to Jiau reference have been fully considered but they are not persuasive.

13. 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., "RFID-contactless interface according to ISO 14443 and ISO 15693 as well as similar interfaces" (p. 24, lines 8-9)) 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). In this case, the Examiner respectfully submits that Jiau has been used to reject claims 1, 8, 18-29 and 31-40, wherein none of the rejected claims recite the above limitation.

#### **Conclusion**

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 maxi-flex.

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). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



Uyen-Chau N. Le  
Primary Examiner  
Art Unit 2876

September 12, 2006

IDS - 04/26/2006

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>	substitute forms PTO/SB/08a & PTO/SB/08b	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
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
UCL	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	
UCL	JJ	US 6,342,839	01-29-2002	Curkendall et al.	

/Uyen Chau Le/  
Examiner Signature

09/12/2006  
Date Considered

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>	substitute forms PTO/SB/08a & PTO/SB/08b	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
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
UCL	f1	DE19631050	02-05-1998	Bergler et al.	Drawings	
	f2	HK 1063994	NO DATE			T
	f3	HK 1063995	NO DATE			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	Scysen	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	Gcmplus	Abs.(Engl), Dwg.	
UCL	f22	WO04 081706	09-23-2004	Digisafe Ltd.		T
UCL	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
UCL	1	ACR38CT Contactless SIM Tracker Technical Specification, Advanced Card Systems Ltd., Hong Kong. NO DATE	T
UCL	2	ACR38DT Dual Key Technical Specifications, Version 1.3, September 2004, Advanced Card Systems Ltd., Hong Kong.	T

/Uyen Chau Le/  
Examiner Signature

09/12/2006  
Date Considered

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>	substitute forms PTO/SB/08a & PTO/SB/08b	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
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-issuc #, publisher, city and/or country where published.	T
UCL	3	Dallas Semiconductor DSI490F 2-in-1 Fob, Dallas Semiconductor, Dallas TX. NO DATE	T
	4	Dallas Semiconductor DS9490R-DS9490B USB to 1-Wire/iButton Adaptor, Maxim I-C, Sunnyvale CA. NO DATE	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. NO DATE	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 Contactless 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
UCL	15	SmartSD Card Structure, Panasonic NO DATE	T

/Uyen Chau Le/  
Examiner Signature

09/12/2006  
Date Considered



**Index of Claims**



Application/Control No.

10/990,296

Examiner

Uyen-Chau N. Le

Applicant(s)/Patent under Reexamination

RYAN ET AL.

Art Unit

2876

√	Rejected
=	Allowed

-	(Through numeral) Cancelled
+	Restricted

N	Non-Elected
I	Interference

A	Appeal
O	Objected

Claim		Date	
Final	Original	9/12/06	
	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	9/12/06	
	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		

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: I.e, Uyen Chau N.  
phone: 571-272-2397  
fax: 571.273-2397

Art Unit: 2876

Dec 14, 2006

**COMMISSIONER FOR PATENTS**

P.O. Box 1450

Alexandria, VA 22313-1450

**AMENDMENT**

This is in response to an Office action, dated September 14, 2006. An interview was scheduled with the Examiner for December 12. The Examiner requested that a proposal be faxed. A proposal was faxed. Applicant's attorney called at exactly 7 minutes past the appointed time. The Examiner was not available for the interview.

In light of this situation (the fact that proposals could not be discussed), it is requested that a subsequent rejection (if any) be made non-final.

## IN THE CLAIMS

### 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; and
  - a contactless interface;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~~ the contactless interface.
  
2. (currently amended) The compact personal token apparatus of claim 1, wherein:
  - 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 ~~appliance~~ appliance is selected from the group consisting of USB, FireWire, IR, Bluetooth, standard serial port, and WLAN, ~~and similar interfaces capable of interfacing with the Internet-capable appliance.~~
  
3. (previously presented) The compact personal token apparatus of claim 1, wherein:
  - the interface with the Internet-capable appliance comprises a USB connection.
  
4. (previously presented) The compact personal token apparatus of claim 1, wherein:
  - 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 14443, ISO 15693, and 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. (currently amended) The compact personal token apparatus of claim 1, wherein:  
the contactless interface is an RFID interface;  
further comprising a wireless interface;  
wherein the translation module moves data or signals from a USB interface to ~~a~~ the  
RFID interface and ~~a~~ to the 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. (previously presented) 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 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. (previously presented) The compact personal token apparatus of claim 12, wherein the  
fob comprises;

a first physical module containing the 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  
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 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, and IBM Micro Drive, ~~and any similar standard interface.~~

22. (currently amended) The compact personal token apparatus of claim 1, further comprising:

a standard-compliant wireless interface selected from the group consisting of Bluetooth compatible interface, WLAN 802.11, and UWB, ~~and any similar interface.~~

23. (previously presented) The compact personal token apparatus of claim 22, further comprising:

a standard-compliant interface releasably 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 802.11device compatible compliant messages, and providing the translation of Bluetooth /WLAN 802.11device compliant messages via a memory chip to standard-compliant contact based interface messages; and

a Bluetooth /WLAN 802.11device having a Bluetooth/WLAN 802.11compliant interface communicating through the interface module with the host processing device via a memory chip; the same Bluetooth /WLAN 802.11device communicating through a Bluetooth /WLAN 802.11compatible interface.

24. (previously presented) The compact personal token apparatus of claim 23, wherein:  
the contactless / wireless interface is releasably 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. (currently amended) 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 ~~the~~ processor module ~~preparing~~ prepares messages to be sent by the ~~contactless/wireless interface~~ contactless and wireless interfaces, and ~~interpreting~~ interprets messages received via the ~~interface~~ contactless and wireless interfaces.

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 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~~ the contactless interface and connected to an inductive antenna.

29. (currently amended) 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. (currently amended) 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. (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, or 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~~ contactless 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, or 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-~~ contactless 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. (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 via a memory chip to Bluetooth /WLAN 802.11device compatible compliant messages, and providing the translation of Bluetooth /WLAN 802.11device compliant messages via a memory chip to standard-compliant contact based interface messages; and

a Bluetooth /WLAN 802.11device having a Bluetooth/WLAN 802.11compliant interface communicating through the interface module with the host processing device via a memory chip; the same Bluetooth /WLAN 802.11device communicating through its Bluetooth/WLAN 802.11compatible 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. (currently amended) 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 including PC, PDA, or 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~~ contactless 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. (currently amended) A compact personal token apparatus, comprising:  
a connection module for interfacing the personal token apparatus with an Internet-capable appliance;  
a contactless interface; and  
a translation module for moving signals between the connection module and the contactless interface;  
wherein the contactless interface is an RFID interface.
54. (currently amended) The apparatus of claim 53 wherein the connection module is selected from the group consisting of USB, FireWire, IR, Bluetooth, standard serial port, and

WI.FAN, ~~and similar~~ interfaces capable of interfacing with the Internet-capable appliance.

55. (original) 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. (currently amended) The apparatus of claim 53 wherein the contactless interface is selected from the group consisting of ISO 14443, ISO 15693, and NFC ~~and similar~~ contactless interfaces.

57. (original) The apparatus of claim 53, further comprising:  
a wireless interface.

58. (original) The apparatus of claim 53, further comprising:  
an RFID or NFC antenna.

59. (original) 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. (currently amended) The method of claim 59, wherein interacting in the real world comprises an activity selected from the group ~~consisting~~ consisting of personal identification, secure network logon, access control, e-ticketing, and e-payment ~~and similar~~ applications.

## REMARKS

### Status

The Office action is responsive to an RCE filed with amendment, responsive to an Office action (final rejection) dated 09/14/2006 .

The Office action is responsive to communication(s) filed on 25 April 2006.

Claim(s) 1-33, 35-48 and 50-60 is/are pending in the application.

Claim(s) 1-33, 35-48 and 50-60 is/are rejected.

A telephonic interview was scheduled for December 12. The Examiner was not available. It is requested that a subsequent rejection (if any) be made non-final.

### *Claim Objections*

In the Office action, Claims 2, 5, 21, 22, 26, 35, 37, 42, 43, 54-56 and 60 are objected to because of use of the word "similar", and appropriate correction is required.

The verbiage involving "similar" is deleted from the claims.

### *Claim Rejections - 35 USC § 102, §103*

Claims 1, 8, 18-29, 31-33 and 35-40 are rejected under 35 U.S.C. 102(e) as being anticipated by **Jiau** (US 2003/0236821 A1).

Claims 1-7, 9, 12-17, 21, 41-48 and 50-60 are rejected under 35 U.S.C. 103(a) as being unpatentable over **Margalit et al** (US 6,748,541) in view of **Weng** (US 6983888 B2).

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.

Claim 30 is rejected under 35 U.S.C. 103(a) as being unpatentable over **Jiau** in view of **Margalit et al**.

### *Traversing the Rejections*

The invention is directed to a device (and method of use) involving:

- contact interface
- contactless interface
- wireless interface

Signals are moved between these various interfaces. For example, information is downloaded from the Internet to the device, via the contact or wireless interfaces, and is later used by the device's contactless interface in a secure real-world transaction.

The **contact interface** may comprise (for example), a USB plug for moving signals to and from a host computer, thereby enabling communication via the Internet with other entities.

The **contactless interface** comprises (for example) an RFID or smart card application such as ISO 14443 , ISO 15693 and NFC.

The **wireless interface** comprises (for example) 802.11, Bluetooth, UWB, WLAN.

Generally, a **wireless interface** is normally simply a substitute for a **contact interface**, enabling devices to be connected over modest distances, such as 10-100 meters, such as for networking in an office environment. In such cases, signals are generally not "moved from" one interface to the other. Signals are moved via the one interface or the other. Situations can also exist (for example) where a machine without a wireless interface is supplied with a dongle that converts (moves signals from) contact (e.g., USB) to wireless (e.g., 802.11).

It has previously been discussed that although **contactless** and **wireless** interfaces both use RF to convey signals, they are completely different interfaces. They are different communications protocols with different capabilities 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 between office computers!

The references cited fail to disclose all of the elements of the invention, and therefore cannot successfully be used to reject the claims, either under §102 (novel) or §103 (non-obvious).

The invention is directed to a device (and method of use) involving various combinations of:

- contact interface
- contactless interface
- wireless interface

The independent claims are 1, 46, 53, 59:

1. A compact personal token apparatus ...
46. Method of interacting wirelessly ...
53. A compact personal token apparatus ...
59. Method of linking the virtual world of the Internet with the real world of contactless transactions ...

The references cited are **Margalit, Jiau, Weng**.

Margalit has

USB interface and  
contains a 7816 smart card chip (Fig. 2, 170)

Margalit does not have a wireless interface.

Margalit does not have a contactless interface.

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.

**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 disclose or suggest a contactless interface.

**Jiau** does not disclose or suggest any smart card functionality.

The Examiner states that **Weng** (newly cited) 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).

The Examiner states that "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 Margalit et al 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 vice versa), and therefore an obvious expedient."

**Applicant disagrees.** Weng discloses portable wireless anti-theft USB device. The device has a portable wireless anti-theft flash memory having a body proper in which there are a flash memory, a high frequency receiver circuit, and a **monode switch to go with a cap**, in



which are a high frequency transmitter, an encoding circuit, and a counter, for casing the body proper. Connecting the body proper to a computing device enables high frequency transmitting, receiving, and **turning on flash memory firewall**. When the transmitting source is a distance away, the firewall becomes engaged thus disabling the flash memory to prevent loss of data from theft for safety purpose.

At Weng, column 1, lines 25-27 "The invention relates to a portable wireless anti-theft USB disc using high frequency transmitting to turn on and off the flash memory firewall to protect from data theft.

In the next paragraph, Weng states "The cap having the transmitting circuit of the aforesaid portable wireless anti-theft USB disc is wearable on user so that when user is close enough to the body proper and to operate the computer, the body proper can receive signals to enable memory firewall. When the cap is away with user from the computer, the memory firewall is disabled from not receiving signals."

Applicant disagrees. Weng does not have "wireless", in the sense of 802.11 or the like, which is a communication interface. Rather, Weng has a simple RF function capable of turning on and off a firewall when in proximity with a selected computer.

Weng does not mention RFID, nor any of the RFID standards, as discussed above. Weng discloses a simple proximity switch, turning a function (firewall) within a portable apparatus on and off depending on distance from a host apparatus.

The present invention utilizes RFID technology to conduct contactless transactions. 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)

Margalit has contact interface (USB) and smart card functionality (7816).

Jiau has a wireless interface for setting up a personal area network (PAN).

Weng has a USB interface, and a simple RF setup for switching a firewall function.

The invention, as claimed, has contact interface (such as USB), plus a contactless interface (such as ISO 14443, ISO 15693, NFC), and the means (translation module) for moving signals between these interfaces. It may also have a wireless interface (such as 802.11) for communicating with a host device in lieu of a contact interface connection, such as for communicating via the Internet for updating applications such as e-ticketing.

More particularly,

**Independent Claim 1** is amended to positively recite "contactless interface" as an element of the claim (whereas, previously, it was referred to indirectly, and may not have been given any patentable weight).

In **claim 4**, the contactless interface comprises a smart card interface.

In **claim 5**, the smart card interface is selected from the group consisting of ISO 14443, ISO 15693 and NFC.

In **claim 10**, the contactless interface is an RFID interface; the device further comprises a wireless interface; and the translation module moves data or signals from a USB interface to the RFID interface and to the wireless interface.

In **claim 11**, the translation module is incorporated in the processor module so that the personal token apparatus can go directly from USB to contactless without being limited by smart card software architecture limitations.

In **claim 22**, a wireless interface is introduced selected from the group consisting of Bluetooth compatible interface, WLAN 802.11 and UWB.

In **claim 27**, the processor module prepares messages to be sent by the contactless and wireless interfaces and interprets messages received via the contactless and wireless interfaces.

In **claim 33**, downloaded information can be used in the real world by using the contactless interface.

**Independent Claim 46** is directed to a method of interacting wirelessly, comprising:

- providing a device;
- interfacing the device with an Internet-capable appliance; and
- providing a contactless interface in the device selected from the group consisting of

ISO 14443 and ISO 15693.

None of the references cited even have a contactless interface!

**Independent Claim 53** is directed to a compact personal token apparatus, comprising:

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

- a contactless interface; and

- a translation module for moving signals between the connection module and the contactless interface;

- wherein the contactless interface is an RFID interface.

None of the references teach or suggest this.

**Independent Claim 59** is directed to a 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.

*Conclusion*

The invention is novel and non-obvious. Applicant has attempted to present reasonable claims, capturing the invention, some of which are highlighted immediately hereinabove.

The Claims should be allowed.

No new matter is entered.

No fee is required.

For the applicant,

/Gerald E. Linden/

Gerald E. Linden  
Reg #30282

/D.A. Stauffer/

Dwight A. Stauffer  
Reg # 47,963

Correspondence via  
Dwight A. Stauffer  
**Customer 37053**

D.A. Stauffer Patent Services I.L.C  
1006 Montford Rd.  
Cleveland Hts. OH 44121  
(216) 381-6599

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	1374161
<b>Application Number:</b>	10990296
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	2050
<b>Title of Invention:</b>	Multi-interface compact personal token apparatus and methods of use
<b>First Named Inventor/Applicant Name:</b>	Dennis J. Ryan
<b>Customer Number:</b>	37053
<b>Filer:</b>	Dwight A. Stauffer
<b>Filer Authorized By:</b>	
<b>Attorney Docket Number:</b>	Ryan C-4
<b>Receipt Date:</b>	14-DEC-2006
<b>Filing Date:</b>	16-NOV-2004
<b>Time Stamp:</b>	12:24:28
<b>Application Type:</b>	Utility

### Payment information:

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

### File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part /.zip	Pages (if appl.)
1		Ryan_C-4_Amd_as_filed_12-14-06.pdf	249806	yes	19

<b>Multipart Description/PDF files in .zip description</b>			
<b>Document Description</b>		<b>Start</b>	<b>End</b>
Amendment - After Non-Final Rejection		1	1
Claims		2	11
Applicant Arguments/Remarks Made in an Amendment		12	19

**Warnings:**

**Information:**

<b>Total Files Size (in bytes):</b>	249806
-------------------------------------	--------

**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.**

## EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L22	842	(235/492,472.02).CCLS.	US-PGPUB	OR	OFF	2007/01/20 14:10
L23	302	22 and @ad<="20031117"	US-PGPUB	OR	ON	2007/01/20 14:23
L25	11	((contact\$1less non\$1contact) and USB and wireless).clm.	US-PGPUB	OR	ON	2007/01/20 14:24

## EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	40	("20010043702" "20010043702" "20010054148" "20010054148" "20020011516" "20030000267" "20030028797" "20030087601" "20030102380" "20030236821" "20030236821" "3941489" "4367965" "5761648" "6067235" "6085320" "6148077" "6148354" "6168077" "6168077" "6189098" "6240184" "6283658" "6342839" "6370603" "6370603" "6385677" "6385677" "6505773" "6543690" "6543690" "6567273" "6567273" "6658516" "6658516" "6676420" "6694399" "6694399" "6724680" "6748541" "6748541" "6752321" "6752321" "6763399" "6763399" "6769499" "6772956" "6772956" "6798169" "6801956" "6801956" "6848045" "6848045" "6876420" "6879597" "6879597" "6983888").PN.	US-PGPUB; USPAT	OR	ON	2007/01/20 13:23
L2	6460	((235/380,375,492) or (705/41,44) or (713/172,200,201)).CCLS.	USPAT	OR	OFF	2007/01/20 14:03
L3	5994	2 and @ad<="20031117"	USPAT	OR	ON	2007/01/20 14:03
L7	3959	3 and @ad>="19950101"	USPAT	OR	ON	2007/01/20 14:03
L9	180	(235/472.02).CCLS.	USPAT	OR	OFF	2007/01/20 14:03
L10	161	9 and @ad<="20031117"	USPAT	OR	ON	2007/01/20 14:11
L11	126	10 and @ad>="19950101"	USPAT	OR	ON	2007/01/20 14:11
S1	13065	usb and (sim smart ic)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/01/18 08:17
S2	6267	contact\$4 and (contact\$1less non\$1contact\$4) and wire\$1less	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/01/18 10:16
S3	527	S1 and S2	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/01/18 08:18
S5	1383928	internet network\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/01/18 09:33



## EAST Search History

S6	489	S3 and S5	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/01/18 08:18
S7	189	S6 and @ad<="20031117"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/01/18 09:34
S8	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	2007/01/18 10:11
S9	2	("6983888").PN.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2007/01/18 09:09
S10	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	2007/01/18 09:09
S11	23	("6307538").PN. OR ("6561421").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/01/18 09:13
S12	7	("6151647"   "6168077"   "6216230").PN. OR ("6763399").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/01/18 09:32
S13	1511	(usb iso contact\$1 contacting) same (contact\$1less noncontact (non adj contact)) same wire\$1less	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/01/18 09:35
S15	1389877	internet network\$4 ethernet	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/01/18 09:34

## EAST Search History

S16	679	S13 and S15	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/01/18 09:36
S17	413	S16 and @ad<="20031117"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/01/18 09:36
S18	149	(usb iso) same (contact\$1less noncontact (non adj contact)) same wire\$1less	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/01/18 09:36
S19	130	S18 and S15	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/01/18 09:36
S20	84	S19 and @ad<="20031117"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/01/18 09:36
S21	8	("5796832"   "5929414"   "6138918"   "6237849"   "6250557"   "6256690"   "6577229").PN. OR ("6776339").URPN.	US-PGPUB; USPAT; USOCR	OR	ON	2007/01/18 09:49
S22	40	("20010043702" "20010043702" "200 10054148" "20010054148" "20020011 516" "20030000267" "20030028797" " 20030087601" "20030102380" "20030 236821" "20030236821" "3941489" "4 367965" "5761648" "6067235" "60853 20" "6148077" "6148354" "6168077" " 6168077" "6189098" "6240184" "6283 658" "6342839" "6370603" "6370603"  "6385677" "6385677" "6505773" "65 43690" "6543690" "6567273" "656727 3" "6658516" "6658516" "6676420" "6 694399" "6694399" "6724680" "67485 41" "6748541" "6752321" "6752321" " 6763399" "6763399" "6769499" "6772 956" "6772956" "6798169" "6801956"  "6801956" "6848045" "6848045" "68 76420" "6879597" "6879597" "698388 8").PN.	US-PGPUB; USPAT	OR	ON	2007/01/18 10:12
S23	7	S22 not S8	US-PGPUB; USPAT	OR	ON	2007/01/18 10:12

## EAST Search History

S24	134503	(triple three multiple plurality) near10 interfac\$4	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/01/18 10:15
S25	93	usb same contact\$4 same (contact\$1less non\$1contact\$4) same wire\$1less	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/01/18 10:16
S26	62	S25 and @ad<="20031117"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2007/01/18 10:17



NOTICE OF ALLOWANCE AND FEE(S) DUE

37053 7590 02/06/2007

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

EXAMINER	
LE, UYEN CHAU N	
ART UNIT	PAPER NUMBER

2876

DATE MAILED: 02/06/2007

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

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

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
-------------	--------------	---------------	---------------------	----------------------	------------------	----------

nonprovisional YES \$700 \$300 \$0 \$1000 05/07/2007

**THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.**

**THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.**

**HOW TO REPLY TO THIS NOTICE:**

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

- A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.
- B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

- A. Pay TOTAL FEE(S) DUE shown above, or
- B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

**IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.**

**PART B - FEE(S) TRANSMITTAL**

**Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE  
 Commissioner for Patents  
 P.O. Box 1450  
 Alexandria, Virginia 22313-1450  
 or Fax (571)-273-2885**

**INSTRUCTIONS:** This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

37053                      7590                      02/06/2007

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

**Certificate of Mailing or Transmission**

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

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

**TITLE OF INVENTION: MULTI-INTERFACE COMPACT PERSONAL TOKEN APPARATUS AND METHODS OF USE**

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	\$700	\$300	\$0	\$1000	05/07/2007

EXAMINER	ART UNIT	CLASS-SUBCLASS
LE, UYEN CHAU N	2876	235-492000

<p>1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).</p> <p><input type="checkbox"/> Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.</p> <p><input type="checkbox"/> "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. Use of a Customer Number is required.</p>	<p>2. For printing on the patent front page, list</p> <p>(1) the names of up to 3 registered patent attorneys or agents OR, alternatively, _____ 1</p> <p>(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. _____ 2</p> <p>_____ 3</p>
--	---

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE \_\_\_\_\_ (B) RESIDENCE: (CITY and STATE OR COUNTRY) \_\_\_\_\_

Please check the appropriate assignee category or categories (will not be printed on the patent):  Individual  Corporation or other private group entity  Government

<p>4a. The following fee(s) are submitted:</p> <p><input type="checkbox"/> Issue Fee</p> <p><input type="checkbox"/> Publication Fee (No small entity discount permitted)</p> <p><input type="checkbox"/> Advance Order - # of Copies _____</p>	<p>4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)</p> <p><input type="checkbox"/> A check is enclosed.</p> <p><input type="checkbox"/> Payment by credit card. Form PTO-2038 is attached.</p> <p><input type="checkbox"/> The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).</p>
---	--

5. Change in Entity Status (from status indicated above)

a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.  b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature \_\_\_\_\_ Date \_\_\_\_\_

Typed or printed name \_\_\_\_\_ Registration No. \_\_\_\_\_

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

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



UNITED STATES PATENT AND TRADEMARK OFFICE

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

Table with columns: 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 02/06/2007
D.A. STAUFFER PATENT SERVICES LLC
1006 MONTFORD ROAD
CLEVELAND HTS., OH 44121-2016
EXAMINER LE. UYEN CHAU N
ART UNIT PAPER NUMBER
2876
DATE MAILED: 02/06/2007

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 0 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 0 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

N

<b>Notice of Allowability</b>	<b>Application No.</b>	<b>Applicant(s)</b>	
	10/990,296	RYAN ET AL.	
	<b>Examiner</b>	<b>Art Unit</b>	
	Uyen-Chau N. Le	2876	

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

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

- 1.  This communication is responsive to 12/14/2006.
- 2.  The allowed claim(s) is/are 1-9, 11-33, 35-48 and 50-60.
- 3.  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 the:
    - 1.  Certified copies of the priority documents have been received.
    - 2.  Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
    - 3.  Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

\* Certified copies not received: \_\_\_\_\_.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application. **THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.**

- 4.  A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
  - 5.  CORRECTED DRAWINGS ( as "replacement sheets") must be submitted.
    - (a)  including changes required by the Notice of Draftsperson's Patent Drawing Review ( PTO-948) attached
      - 1)  hereto or 2)  to Paper No./Mail Date \_\_\_\_\_.
    - (b)  including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date \_\_\_\_\_.
- Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).
- 6.  DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

**Attachment(s)**

- 1.  Notice of References Cited (PTO-892)
- 2.  Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3.  Information Disclosure Statements (PTO/SB/08),  
Paper No./Mail Date \_\_\_\_\_
- 4.  Examiner's Comment Regarding Requirement for Deposit of Biological Material
- 5.  Notice of Informal Patent Application
- 6.  Interview Summary (PTO-413),  
Paper No./Mail Date 20070120.
- 7.  Examiner's Amendment/Comment
- 8.  Examiner's Statement of Reasons for Allowance
- 9.  Other \_\_\_\_\_.

**EXAMINER'S AMENDMENT**

***Prelim. Amdt/Amendment***

1. Receipt is acknowledged of the Amendment filed 12/14/2006.
2. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this examiner's amendment was given in a telephone interview with Mr. Linden and Mr. Finn on 18 January 2007 in order to place the instant application in the proper form for an allowance by incorporating the limitation of claim 10 into each of the independent claims and deleting the phrase "similar" recited in claim 55.

The application has been amended as follows:

Re claim 1: Please substitute claim 1 with following:



Art Unit: 2876

1. A compact personal token apparatus, comprising:

- a connection module;
  - a translation module;
  - a processor module;
  - an input/output module; and
  - a contactless interface;
- 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 the contactless interface;

wherein:

the contactless interface is an RFID interface;

further comprising a wireless interface;

wherein the translation module moves data or signals from a USB interface to the RFID interface and to the 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.

Re claim 10: Please cancel claim 10 without prejudice and/or traverse.

Re claim 46: Please substitute claim 46 with the following:

Art Unit: 2876

46. Method of interacting wirelessly, comprising:  
providing a device;  
interfacing the device with an Internet-capable appliance; and  
providing a contactless interface in the device selected from the group consisting of  
ISO 14443 and ISO 15693;  
wherein the contactless interface is an RFID interface;  
further comprising providing a wireless interface;  
wherein the translation module moves data or signals from a USB interface to the  
RFID interface and to the 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.

Re claim 53: Please substitute claim 53 with the following:

53. A compact personal token apparatus, comprising:  
a connection module for interfacing the personal token apparatus with an Internet-  
capable appliance;  
a contactless interface; and  
a translation module for moving signals between the connection module and the  
contactless interface;  
wherein the contactless interface is an RFID interface;  
further comprising a wireless interface;  
wherein the translation module moves data or signals from a USB interface to the  
RFID interface and to the 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.

Re claim 55: Please substitute claim 55 with the following:

Art Unit: 2876

55. The apparatus of claim 53 wherein the Internet-capable appliance is selected from the group consisting of personal computer (PC), laptop, PDA, MP3 player, and cellphone, ~~and similar Internet-capable devices.~~

Re claim 59: Please substitute claim 59 with the following:

59. 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;

further comprising providing a wireless interface:

wherein the translation module moves data or signals from a USB interface to the RFID interface and to the 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.

*Allowable Subject Matter*

3. Claims 1-9, 11-33, 35-48 and 50-60 are allowed.

4. The following is an examiner's statement of reasons for allowance:

Art Unit: 2876

The prior art of records to Margalit which discloses a USB interface and a contact interface (i.e., 7816 smart card), Jiau which discloses a USB interface and a wireless interface, Weng which discloses a wireless USB device and all other cited references, taken alone or in combination, fails to teach or fairly suggest the specific structure and/or the method a personal token apparatus comprising, among other things, a USB interface, a contactless interface which is an RFID interface, and a wireless interface, wherein the translation module move data or signals from the USB interface to the RFID interface and to the 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 as set forth in the claimed combinations.

#### **Conclusion**

Any comments considered necessary by applicant must be submitted no later than the payment of the issue fee and, to avoid processing delays, should preferably accompany the issue fee. Such submissions should be clearly labeled "Comments on Statement of Reasons for Allowance."

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Uyen-Chau

Art Unit: 2876

N. Le whose telephone number is 571-272-2397. The examiner can normally be reached on M-F 5:30AM-2PM.

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). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



Uyen-Chau N. Le  
Primary Examiner  
Art Unit 2876

January 20, 2007

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

All participants (applicant, applicant's representative, PTO personnel):

- (1) Uyen-Chau N. Le. (3) David Finn (inventor).  
(2) Gerald E. Linden (Reg. 30282). (4) \_\_\_\_\_.

Date of Interview: 18 January 2007.

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 and Mr. Finn authorized an Examiner amendment in order to place the instant application in the proper form for an allowance by incorporating the limitation of claim 10 into each of the independent claims and deleting the phrase "similar" recited in claim 55.

(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.

  
**MICHAEL G. LEE**  
**SUPERVISORY PATENT EXAMINER**  
**TECHNOLOGY CENTER 2800**

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.

<b>Issue Classification</b> 	<b>Application/Control No.</b> 10990296	<b>Applicant(s)/Patent Under Reexamination</b> RYAN ET AL.
	<b>Examiner</b> Le, Uyen-Chau N	<b>Art Unit</b> 2876

ORIGINAL				INTERNATIONAL CLASSIFICATION										
CLASS		SUBCLASS		CLAIMED				NON-CLAIMED						
235		492		G	0	6	K	19/06						
<b>CROSS REFERENCE(S)</b>														
CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)													
235	472.02													

NONE (Assistant Examiner)	(Date)					<b>Total Claims Allowed:</b> 57			
<i>Alex Joubert</i> (Legal Instruments Examiner)	2/15/07 (Date)	UYEN-CHAU N. LE (Primary Examiner)	<i>Uchaulé</i> (Date)	1/20/07 (Date)	<b>O.G. Print Claim(s)</b> 1		<b>O.G. Print Figure</b> 3B		



<b>Index of Claims</b>  	<b>Application/Control No.</b>  10990296	<b>Applicant(s)/Patent Under Reexamination</b>  RYAN ET AL.
	<b>Examiner</b>  Le, Uyen-Chau N	<b>Art Unit</b>  2876

✓	<b>Rejected</b>
=	<b>Allowed</b>


-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

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

CLAIM		DATE									
Final	Original	01/20/2007									
1	1	=									
2	2	=									
3	3	=									
4	4	=									
5	5	=									
6	6	=									
7	7	=									
8	8	=									
9	9	=									
	10	-									
10	11	=									
11	12	=									
12	13	=									
13	14	=									
14	15	=									
15	16	=									
16	17	=									
17	18	=									
18	19	=									
19	20	=									
20	21	=									
38	22	=									
39	23	=									
40	24	=									
41	25	=									
42	26	=									
43	27	=									
21	28	=									
22	29	=									
23	30	=									
24	31	=									
25	32	=									
26	33	=									
	34	-									
27	35	=									
28	36	=									

<b>Index of Claims</b> 	<b>Application/Control No.</b> 10990296	<b>Applicant(s)/Patent Under Reexamination</b> RYAN ET AL.
	<b>Examiner</b> Le, Uyen-Chau N	<b>Art Unit</b> 2876

✓	<b>Rejected</b>
=	<b>Allowed</b>

-	<b>Cancelled</b>
÷	<b>Restricted</b>

N	<b>Non-Elected</b>
I	<b>Interference</b>

A	<b>Appeal</b>
O	<b>Objected</b>

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

CLAIM		DATE									
Final	Original	01/20/2007									
29	37	=									
30	38	=									
31	39	=									
32	40	=									
33	41	=									
34	42	=									
35	43	=									
36	44	=									
37	45	=									
44	46	=									
45	47	=									
46	48	=									
	49	-									
47	50	=									
48	51	=									
49	52	=									
50	53	=									
51	54	=									
52	55	=									
53	56	=									
54	57	=									
55	58	=									
56	59	=									
57	60	=									

<b>Search Notes</b>	Application/Control No.	Applicant(s)/Patent Under Reexamination
	Examiner	Art Unit

<b>SEARCHED</b>			
<b>Class</b>	<b>Subclass</b>	<b>Date</b>	<b>Examiner</b>

<b>SEARCH NOTES</b>		
<b>Search Notes</b>	<b>Date</b>	<b>Examiner</b>

<b>INTERFERENCE SEARCH</b>			
<b>Class</b>	<b>Subclass</b>	<b>Date</b>	<b>Examiner</b>



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 \*\*\*\*\* *MM*

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 \*\*\*\*\* *MM*

IF REQUIRED, FOREIGN FILING LICENSE GRANTED  
 \*\* 12/16/2004

\*\* SMALL ENTITY \*\* *MM*

Foreign Priority claimed <input type="checkbox"/> yes <input checked="" type="checkbox"/> no	STATE OR COUNTRY AZ	SHEETS DRAWING 4	TOTAL CLAIMS 52	INDEPENDENT CLAIMS 3
35 USC 119 (a-d) conditions met <input type="checkbox"/> yes <input checked="" type="checkbox"/> no <input type="checkbox"/> Met after Allowance				
Verified and Acknowledged Examiner's Signature <i>MM</i> Initials				

ADDRESS

37053  
 D.A. STAUFFER PATENT SERVICES LLC  
 1006 MONTFORD ROAD  
 CLEVELAND HTS. , OH  
 44121-2016

TITLE

Multi-interface compact personal token apparatus and methods of use

FILING FEE	FEES: Authority has been given in Paper	<input type="checkbox"/> All Fees
		<input type="checkbox"/> 1.16 Fees ( Filing )
		<input type="checkbox"/> 1.17 Fees ( Processing Ext. of time )

10/990, 296

LR  
2/26/07

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 <sup>5</sup>6.**

LR  
2/26/07

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

**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 <sup>22</sup>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

<b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>	substitute forms PTO/SB/08a & PTO/SB/08b	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/
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
UCL	f1	DE19631050	02-05-1998	Bergler et al.	Drawings	
	f2	HK 1063994	<del>NO DATE</del>	12/2004		T
	f3	HK 1063995	<del>NO DATE</del>	12/2004		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	Scysen	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
UCL	f23	WO04 081769	09-24-2004	Axalto SA		T

D8  
2/26/07

**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
UCL	1	ACR38CT Contactless SIM Tracker Technical Specification, Advanced Card Systems Ltd., Hong Kong. NO DATE	T
UCL	2	ACR38DT Dual Key Technical Specifications, Version 1.3, September 2004, Advanced Card Systems Ltd., Hong Kong.	T

/Uyen Chau Le/  
Examiner Signature

09/12/2006  
Date Considered



substitute forms <b>PTO/SB/08a</b> & <b>PTO/SB/08b</b>  <b>INFORMATION DISCLOSURE STATEMENT BY APPLICANT</b>	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 <del>f</del>
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
<i>WU</i>	A	US-3,941,489	<del>03-22-1974</del>	Bryan <i>3/1976</i>	
	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	Hoomaert	
	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	

*28*  
*31107*



**PART B - FEE(S) TRANSMITTAL**

Complete and send this form, together with applicable fee(s), to: **Mail** Mail Stop ISSUE FEE  
 Commissioner for Patents  
 P.O. Box 1450  
 Alexandria, Virginia 22313-1450  
 or **Fax** (571)-273-2885

**INSTRUCTIONS:** This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

37053 7590 02/06/2007

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

**Certificate of Mailing or Transmission**  
 I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop (ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

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

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

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	\$700	\$300	\$0	\$1000	05/07/2007

EXAMINER	ART UNIT	CLASS-SUBCLASS
LE, UYEN CHAUN	2876	235-492000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363)

- Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
- "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev. 03-02 or more recent) attached. Use of a Customer Number is required.

2. For printing on the patent front page, list  
 (1) the names of up to 3 registered patent attorneys or agents OR, alternatively,  
 (2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1. Gerald E. Linden  
 2. Dwight A. Stauffer  
 3. X

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: DPD Patent Trust Ltd  
 (B) RESIDENCE (CITY and STATE OR COUNTRY): Lower Churchfield, Tourmakeady, Co. Mayo, IRELAND

Please check the appropriate assignee category or categories (will not be printed on the patent):  Individual  Corporation or other private group entity  Government

4a. The following fee(s) are submitted.

- Issue Fee
- Publication Fee (No small entity discount permitted)
- Advance Order - # of Copies \_\_\_\_\_

4b. Payment of Fee(s) (Please first reapply any previously paid issue fee shown above)

- A check is enclosed.
- Payment by credit card. Form PTO-2038 is attached.
- The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number \_\_\_\_\_ (enclose an extra copy of this form).

Paying via EFS

5. Change in Entity Status (From status indicated above)

- a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.
- b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant, a registered attorney or agent, or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature: Gerald E. Linden  
 Typed or printed name: Gerald E. Linden

Date: 30 March 2007  
 Registration No.: 30,282

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450

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

## Electronic Patent Application Fee Transmittal

<b>Application Number:</b>	10990296
<b>Filing Date:</b>	16-Nov-2004
<b>Title of Invention:</b>	MULTI-INTERFACE COMPACT PERSONAL TOKEN APPARATUS AND METHODS OF USE
First Named Inventor/Applicant Name:	Dennis J. Ryan
<b>Filer:</b>	Gerald Linden
<b>Attorney Docket Number:</b>	RYAN C-4

Filed as Small Entity

### Utility Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
<b>Basic Filing:</b>				
<b>Pages:</b>				
<b>Claims:</b>				
<b>Miscellaneous-Filing:</b>				
<b>Petition:</b>				
<b>Patent-Appeals-and-Interference:</b>				
Post-Allowance-and-Post-Issuance:				
Utility Appl issue fee	2501	1	700	700
Publ. Fee- early, voluntary, or normal	1504	1	300	300

IPR2022-00412

Description	Fee Code	Quantity	Amount	Sub-Total in USD(\$)
Extension-of-Time:				
Miscellaneous:				
<b>Total in USD (\$)</b>				<b>1000</b>

## Electronic Acknowledgement Receipt

<b>EFS ID:</b>	1638989
<b>Application Number:</b>	10990296
<b>International Application Number:</b>	
<b>Confirmation Number:</b>	2050
<b>Title of Invention:</b>	MULTI-INTERFACE COMPACT PERSONAL TOKEN APPARATUS AND METHODS OF USE
<b>First Named Inventor/Applicant Name:</b>	Dennis J. Ryan
<b>Customer Number:</b>	69186
<b>Filer:</b>	Gerald Linden
<b>Filer Authorized By:</b>	
<b>Attorney Docket Number:</b>	RYAN C-4
<b>Receipt Date:</b>	30-MAR-2007
<b>Filing Date:</b>	16-NOV-2004
<b>Time Stamp:</b>	09:44:05
<b>Application Type:</b>	Utility

### Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	\$ 1000
RAM confirmation Number	1691
Deposit Account	

### File Listing:

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

1	Issue Fee Payment (PTO-85B)	efs_c4_issue_fee_transmittal.pdf	89780	no	1
---	-----------------------------	----------------------------------	-------	----	---

Warnings:

Information:

2	Fee Worksheet (PTO-06)	fee-info.pdf	8305	no	2
---	------------------------	--------------	------	----	---

Warnings:

Information:

<b>Total Files Size (in bytes):</b>			98085		
-------------------------------------	--	--	-------	--	--

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

**New Applications Under 35 U.S.C. 111**

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

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

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

**New International Application Filed with the USPTO as a Receiving Office**

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



APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/990,296	05/08/2007	7213766	RYAN C 4	2050

69185 7590 04/18/2007  
LINDEN, STAUFFER PATENTS  
1006 MONTFORD RD.  
CLEVELAND HTS., OH 44121

### ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

#### Determination of Patent Term Adjustment under 35 U.S.C. 154 (b) (application filed on or after May 29, 2000)

The Patent Term Adjustment is 0 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (<http://pair.uspto.gov>).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site <http://pair.uspto.gov> for additional applicants):

Dennis J. Ryan, Chandler, AZ;  
David Finn, Mayo, IRELAND;  
Patrick R. Comiskey, University Heights, OH;  
Norbert Knapich, Rosshaupten, GERMANY;



APPLICATION NUMBER	PATENT NUMBER	GROUP ART UNIT	FILE WRAPPER LOCATION
10/990,296	7213766	2876	9200

## Correspondence Address / Fee Address Change

The following fields have been set to Customer Number 69186 on 03/23/2007

- Correspondence Address
- Maintenance Fee Address

The address of record for Customer Number 69186 is:

LINDEN, STAUFFER PATENTS  
1006 MONTFORD RD.  
CLEVELAND HTS., OH 44121