Fig. 19 is a flow diagram illustrating an example implementation of a primary routine that may be executed by the controller(s) of the network server(s) shown in Fig. 4;

Fig. 20 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO REGISTER NEW POCKET VAULT HOLDER routine shown in Fig. 19;

Fig. 21 is a flow diagram illustrating an example implementation of the PROCESS REQUEST BY MEDIA ISSUER/ADVERTISER TO UPDATE NETWORK SERVER routine shown in Fig. 19;

Fig. 22 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO UPDATE INFO ON POCKET VAULT routine shown in Fig. 19;

Fig. 23 is a flow diagram illustrating an example implementation of the PROCESS REQUEST FROM HOLDER TO LOAD NEW FILE ONTO NETWORK SERVER routine shown in Fig. 19;

Fig. 24 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO AUTHORIZE TRANSACTION routine shown in Fig. 19;

Fig. 25 is a flow diagram illustrating an example implementation of the AUTHORIZED POCKET VAULT USE? routine shown in each of Figs. 20, 22, and 24; and

Figs 26a-26p are illustrations of the portable electronic authorization device, as well as the token (e.g., a card) associated therewith, as these items may appear when in use;

Fig. 27 is a block diagram illustrating several additional features that may optionally be added to a network system such as that shown in Fig. 1 so as to enhance the functionality of the network;

Fig 28 is a block diagram illustrating example components that may optionally be added to software executing on a controller of the Pocket Vault, such as the software described in connection with Figs. 7-12, so as to enhance the functionality of the Pocket Vault in a network environment;

Fig 29 is a data flow diagram illustrating an example of how data may flow between the Pocket Vault and a user interface of an interface station computer to which the Pocket Vault is interfaced/docked;

Fig. 30 is a flow diagram illustrating an example of a primary routine that may be executed by a website on the network server(s) shown in Fig. 27, which website may be accessed, for example, by a browser executing on the interface station computer shown in Fig. 27;

Fig. 31 is a flow diagram illustrating an example implementation of the INSTALL DRIVER(S) routine shown in Fig. 30;

Fig. 32 is a flow diagram illustrating an example implementation of the NEW POCKET VAULT HOLDER routine shown in Fig. 30;

Fig. 33 is a flow diagram illustrating an example implementation of the EXISTING POCKET VAULT HOLDER routine shown in Fig. 30;

Fig. 34 is a flow diagram illustrating an example implementation of the CARD LOADING routine shown in Fig. 33;

Fig. 35 is a flow diagram illustrating an example implementation of the SYNCHRONIZATION routine shown in Fig. 33;

Fig. 36 is a flow diagram illustrating an example implementation of the RECOVERY routine shown in Fig. 33;

Fig. 37 is a flow diagram illustrating an example implementation of the IDENTITY PORTING SELECTION routine shown in Fig. 33;

Fig. 38 is a flow diagram illustrating an example implementation of the BACKUP routine shown in Fig. 33; and

Fig. 39 is a flow diagram illustrating an example implementation of the SET PREFERENCES routine shown in Fig. 33.

DETAILED DESCRIPTION

A new method and system for producing, distributing, storing, and using the typical contents of an individual's wallet is disclosed herein. Essentially, the system may enable individuals to replace nearly all of the paper and plastic contents of their wallets with a single, hand-held portable electronic authorization device. The system may include the portable electronic authorization devices, removable morphing tokens or cards associated with such devices, associated computer peripherals, software and certain network capabilities. As a whole, the system may eliminate virtually all of the distribution costs and security concerns associated with paper and plastic media.

Because the device may incorporate many different media that are commonly stored in a person's wallet, possibly including both financial and non-financial media, it is much more than a simple point-of-sale (POS) device. Therefore, the device may be more appropriately referred to as a multi-purpose, "point-of-transaction" device. In any situation

of presentment, whether for purposes such as building security, demonstrating membership or using credit or debit capacity, the system is designed to perform tasks more safely, securely and with greater ease than is possible with prior art systems. Further, while certain computer technologies are involved, the preferred embodiment is such that some people may barely recognize it as a computer, seeing instead a more comfortable to carry, easier-to-use, safer and more securely packaged means of transporting typical wallet contents.

The system's business model may comprise an independent organization acting as a media-neutral, multi-service provider of other issuers' various financial and non-financial media, that also may enable individuals and retailers to add or create their own secure (and where appropriate, non-secure media) using a device with a self-contained set of authentication security features, which may even be password-free. This device may operate over existing financial transaction networks, while also having links to a highly secure network system for certain functionality. The self-contained authentication functionality of the device itself ensures privacy, while providing sufficient accountability/traceability to satisfy law enforcement concerns.

A network system 100 configured according to one illustrative embodiment of the invention is shown in Fig. 1. As shown, the network system 100 may include a portable electronic authorization device 102 (alternatively referred to herein as a "Pocket Vault") and an associated token 102a (alternatively referred to herein as a "Chameleon Card"). Each person desiring to use the network system 100 may possess his or her own the Pocket Vault 102 and associated token 102a. Some individuals may choose to own multiple Pocket Vaults or Chameleon Cards. The system and software therefore may accommodate the use of multiple Pocket Vaults and multiple Chameleon Cards by one individual.

Referring to Fig. 1, in addition to the Pocket Vault 102, the network system 100 may include one or more network servers 114 to which various other network components are coupled. Although multiple, load-sharing network servers 114 may be employed in a typical application, the network server(s) 114 will hereinafter, for convenience, occasionally be referred to as a single network server 114. Coupled to the network server 114 are: several different types of interface stations 104 (i.e., a validation interface station 104a , a personal interface station 104b, and a commercial interface station 104c), one or more commercial card readers 106, one or more commercial bar code readers 107, and several computers 108, 110, and 112 operated by one or more advertisers, non-financial media issuers, and financial

media issuers, respectively. The structure and functionality of each of the components of the network system 100 in accordance with illustrative embodiments of the invention are described below.

As shown in Fig. 1, the network server 114 may form the hub of the network system 100, with each of the interface stations 104, the commercial card reader 106, the commercial bar code reader 107, and the computers 108, 110, and 112 being coupled thereto. As discussed in more detail below, the network server 114 may therefore serve as: (1) a repository of information for the network, (2) the entity that controls access to the stored information by the other network devices, and (3) a service provider for financial and non-financial media issuers, advertisers, as well as Pocket Vault holders.

Any of a number of techniques may be used to interconnect the various elements of the network system 100, and the invention is not limited to any particular networking technique. In one illustrative embodiment, for example, the network server 114 is coupled to the other elements in the network system 100 via the Internet or similar packet-switched communication system. Alternatively, dedicated or selectively established (e.g., using a dial-up modem) communication channels or time slots thereof may be employed between the respective devices. The connections between the network devices may be either hardwired (including fiber optic connections) or wireless (e.g., infrared (IR) or radio frequency (RF) links).

As shown in Fig. 1, the Pocket Vault 102 may be interfaced with any of the interface stations 104a-c so as to permit information to be uploaded from the network server 114 to the Pocket Vault 102, or to be downloaded from the Pocket Vault 102 to the network server 114. In one illustrative embodiment, each of the interface stations 104 includes a docking mechanism that permits a Pocket Vault 102 to be physically, as well as electronically, interfaced therewith. In such an embodiment, once the Pocket Vault 102 is physically "docked" with an interface station 104, the Pocket Vault 102 may communicate with the interface station 104 using any now known or later discovered technique. For example, physical contact may be made between respective electrodes or plugs, a line of sight (e.g., infrared) wireless link may be established, or any other interfacing technique may be employed.

The Pocket Vault 102 may additionally or alternatively be configured such that it need not be physically docked with or even in the same room as the interface station 104, as a

wireless network such as Bluetooth may be employed to permit communication between devices on the network system 100. In fact, in some embodiments wherein appropriate networking capabilities are provided, each Pocket Vault 102 may communicate directly with the network server 114, without the interface stations 104a-c facilitating communication therebetween. In addition, in some embodiments, Pocket Vaults 102 may communicate directly with one another. In such embodiments, such inter-device communication may permit value to be exchanged directly between Pocket Vaults 102.

The personal docking station 104b may allow setting or changing of user preferences, recording of miscellaneous information by the Pocket Vault holder, replenishment or deletion of information regarding particular media, and may also permit additional media (e.g., a library card) to be added to the device. The Pocket Vault holder may, for example, directly add non-value-based media (e.g., a membership number for the local Historical Society) and notes to the Pocket Vault 102. In one embodiment, value-based and certain identification media (a driver's license, passport, building security ID, etc.) may be added or reinstated only through a secure connection to the network server 114 (as described below), in response to an update request from the Pocket Vault holder. In addition, the personal interface station may provide a mechanism to download transaction activity involving the Pocket Vault 102 into an individual's home computer. There are many users of home finance software. These applications can be relatively "data hungry," and commonly require users to download checking and debit card data from their banks (or key it in manually) and to key in the details of credit card and cash purchases. All of this keying and internet file downloading from third parties may be replaced by a simple docking procedure, i.e., when the Pocket Vault 102 is interfaced with the personal docking station 102b.

As shown in Fig. 1, and as described below in more detail, the Pocket Vault 102 may be equipped to generate the token 102a such that the token 102a has transactional information regarding a media (e.g., a simulated magnetic stripe or a bar code) produced thereon. In such an embodiment, after the token 102a has been generated, the token 102a may be used by the Pocket Vault holder to engage in a transaction wherein an entity swipes the simulated magnetic stripe of the token 102a through a card reader 106 or scans the bar code on the token 102a using a bar code reader 107. Additionally or alternatively, the token 102a may include a suitable Smartcard interface so that the Chameleon Card 102 may be used with Smartcard compatible devices.

Because the token 102a may be caused to take on a different personality each time it is released from the Pocket Vault 102, a plurality of media may be stored electronically in memory of the Pocket Vault 102, and the token 102a may, upon request, be generated to take on the personality selected by the Pocket Vault holder. The respective media stored on the Pocket Vault 102 may be issued by different and unrelated media issuers. As used herein, two media issuers are "unrelated" if there exists no legal relationship between them. The token 102a may also have display capacity, sufficient to indicate the media personality that it has taken on. This may or may not include display of the specific identity that is temporarily encoded on the token 102a. In some embodiments, value may be exchanged between two Pocket Vaults 102 when one the Pocket Vault 102 generates a token 102a having a value-based or value-linked media stored thereon, and the token 102a so generated is passed to the other the Pocket Vault 102, which then may then access the media and extract value therefrom or add value thereto. As mentioned above, this sort of value exchange may also be accomplished directly between two Pocket Vaults 102 over a wireless network, such as Bluetooth.

As discussed in more detail below, in addition to or in lieu of the token 102a, the Pocket Vault 102 may also generate a bar code for a selected media on the Pocket Vault's display (not shown in Fig. 1), and the bar code reader 107 may be used to scan the displayed bar code to process a transaction. Further, a transaction may be processed via a commercial interface station 104c either by use of a docking terminal or via a wireless network scheme such a Bluetooth. In one embodiment, some commercial interface stations 104c may comprise an interface station linked to a standard commercial card reader 106 or commercial bar code reader 107, with the card reader 106 or bar code reader 107 being modified to accept input from the station.

To permit the Pocket Vault holder to select from among the various media stored in memory of the Pocket Vault 102, the Pocket Vault 102 may comprise a display (not shown in Fig. 1). By employing either a display having a user-manipulable touch screen or a separate user input device (not shown in Fig. 1), a Pocket Vault holder can effectively flip through the contents of the Pocket Vault 102 to locate and select a desired media (e.g., a credit card, driver's license, library card, frequent flier card, etc.) much like a person can flip through the contents of his or her wallet to do the same.

The use of a display on the Pocket Vault 102 also creates an opportunity for media providers to go from a static presentation of their brand (logo, etc.) to having the option of dynamic branding and messaging. In addition, using the display, the presentment of active marketing at the "moment of buying decision" is possible. Specifically, the logo and message displayed to the Pocket Vault holder may incorporate motion, moving images and messages. To conserve power, moving images may be presented only at certain times, e.g., in response to internal or external events or communications.

In the embodiment of Fig. 1, the computers 108, 110, and 112, together with the network server 114, may represent a secure infrastructure of server databases capable of storing information for purposes of delivering personalized services to holders of Pocket Vaults 102. The network server 114 may also track activity of Pocket Vault holders and compile marketing information based thereupon that may prove useful to media issuers and/or advertisers. The Pocket Vault holder may have control over the ability of the network server 114 to track activity. The information maintained on the network system 100 may originate with the holders of Pocket Vaults 102 and/or may originate with the other entities having access to the network system 100 (e.g., advertisers and media issuers).

As discussed below in more detail, in some embodiments of the invention, certain uses of the Pocket Vault 102, as well as each of the interface stations 104a-c, may be permitted only by pre-authorized individuals. To this end, a suitable user authentication technique may be employed in connection with each attempted use of any of these devices. One suitable user authentication technique that may be employed is the analysis of a bio-metric feature of the individual attempting use of the device (e.g., a fingerprint scan, retina scan, a speech pattern analysis, keystroke rhythm, etc.), and validating the identity of the individual on that basis. Alternatively or additionally, a personal identification (PIN) code may be entered by the holder to verify the holder's identity. In one illustrative embodiment, authentication information used to validate the holder's identity (e.g., the stored fingerprint and/or PIN code) is stored within the to-be-accessed device, and the validation is performed in its entirety on-board the same device, such that the user-specific authentication information never leaves the device in which it is stored. Thus, using this technique, the likelihood that such information will be intercepted by unauthorized third parties may be reduced significantly.

It should be appreciated that, for some applications, it may be desirable to receive and store authentication information (e.g., fingerprint data) of some or all Pocket Vault holders in the network server 114. Accordingly, in some embodiments, such authentication information may be maintained by the network server 114. This authentication information may be transmitted to the network server 114, for example, when Pocket Vaults 102 are first validated.

As discussed below, great care may be taken to ensure that only authorized individuals are permitted to validate Pocket Vaults 102 by having their authentication information (e.g., their fingerprint data or PIN codes) stored therein. Therefore, after it has been confirmed that the holder's authentication information has been properly stored in the Pocket Vault 102, a trust relationship may be established between the network server 114 and the Pocket Vault 102. This relationship may involve, for example, the registration of a unique encrypted chip ID of the Pocket Vault 102 with the network server 114 through a secure Internet connection, the distribution of a digital certificate (e.g., a PKI certificate) to the Pocket Vault 102, and the grant of authority to the Pocket Vault 102 to permanently store the Pocket Vault holder's authentication information.

A similar level of care may also be taken to ensure that only authorized individuals are permitted to validate interface stations 104a-c by having their authentication information (e.g., their fingerprint data or PIN codes) stored therein. Therefore, as with the Pocket Vaults 102, after it has been confirmed that each interface station's authorization information has been properly stored in the interface station 104, a trust relationship may be set up between the network server 114 and the interface station 104. This relationship may also involve, for example, the registration of a unique encrypted chip ID of the interface station 104 with the network server 114 through a secure Internet connection, the distribution of a digital certificate to the interface station 104, and the grant authority to the interface station 104 to permanently store the interface station operator's authentication information. While, in some embodiments, the Pocket Vault 102 and/or the interface stations 104 are each permitted to store authentication information for only one individual, it should be appreciated that, in alternative embodiments, the Pocket Vault 102 and/or the interface stations 104 may each store authentication information for more than one individual, thereby permitting multiple people to use them.

Because of the creation of the above-described trust relationships, each Pocket Vault 102 and each interface station 104 may communicate securely with the network server 114, as well as with any other networked devices or sites that require a high level of trust. Also, the existence of these trust relationships enable individual Pocket Vaults 102 to accept other services provided by the network servers 114, such as the backup and recovery of information stored within the Pocket Vaults 102. That is, the network servers 114 can serve as a repository for all of the information stored on every validated Pocket Vault 102 (except the holder's authentication information – which, in some embodiments, is stored only in the Pocket Vault 102). To ensure that the network server 114 stores an accurate version of the contents of each Pocket Vault 102, information may, for example, be uploaded from the network server 114 to a Pocket Vault 102 or downloaded from the Pocket Vault 102 to the network server 114 each time the Pocket Vault 102 is interfaced with any of the interface stations 104a-c. Therefore, if a Pocket Vault 102 is lost or stolen, the Pocket Vault holder need only obtain a new Pocket Vault 102, and the entire contents of the lost Pocket Vault 102 can be uploaded thereto, in a single communication, in a matter of seconds. In addition, in the event that a validated Pocket Vault 102 is lost or stolen, the network server 114 may void the chip ID of that Pocket Vault 102, so that the Pocket Vault 102 cannot be used by a third party, even if the holder validation security (e.g., the bio-metric scanning or PIN entry requirement) is somehow breached. Voiding the chip ID of the Pocket Vault 102 may, for example, prevent the Pocket Vault 102 from assigning any media information to the associated Chameleon Card.

In addition to serving as a repository for Pocket Vault information, the network server 114 may also serve as a repository for information regarding media issuers or advertisers, and may further provide various services to these entities. For example, the network server 114 may facilitate transactions involving media issued by media issuers, and may permit new media to be issued or lost media to be replaced at a fraction of the cost of generating new physical tokens or replacing lost ones. Additionally, the network server 114 may serve as a conduit for advertisers to target particular classes of Pocket Vault holders, and channel information to them. The network server 114 may also function as an advocate for Pocket Vault holders, advertisers, and/or media issuers when it utilizes its portfolio of Pocket Vault holders, media issuers, and/or advertisers to secure privileges. Examples of such advocacy include the ability to secure buying power for Pocket Vault holders as a group or to provide

media issuers and advertisers with a highly efficient tool for generating awareness for affinities or causes that fit appropriate holder markets. In sum, the services provided by the network server 114 enable Pocket Vault holders to combine and manage their media data using a single, hand-held device, and enables advertisers and media issuers to understand more about, and more readily reach more of, their customers than ever before.

Fig. 2 shows an example embodiment of the Pocket Vault 102 of Fig. 1. The Pocket Vault 102 may employ components similar to those used in modern personal digital assistants (PDAs) and palm top computers. Examples of such products include PDAs such as the "Palm Pilot" from Palm, Inc. (www.palm.com), and the "Casiopedia" from Casio, Inc. of Dover, New Jersey (www.casio.com). As shown, the Pocket Vault 102 may include a controller 202, as well as a transceiver 204, a user input device 206, a docking interface 208, a read/write memory 210, a write-once memory 212, a power manager 214, an indicator 215, a display 216, a token port 218, and a fingerprint scanner 220, all coupled to the controller 202. In addition, the Pocket Vault 102 may include a hard-wired memory (not shown) to store device serial numbers and key operating system and encryption software components.

Actual views of an example embodiment of the Pocket Vault 102, as well as the token 102a associated therewith, are shown in Figs. 26A-26P. The views of Figs. 26A-P, including the items displayed on the display 216, are discussed in more detail below in connection with the flow diagrams of Figs. 7-12. At this point, however, with reference to Figs. 26A-L and 26O, it may be noted that the Pocket Vault 102 may comprise a housing 2602 in which the components shown in Fig. 2 may be disposed. As illustrated in Figs. 26E and 26F, the housing 2602 may be approximately seventy millimeters wide, approximately one hundred millimeters long, and approximately fifteen millimeters deep. Thus, in the embodiment shown, the housing 2602 has an internal volume of less than 105 cubic centimeters. Of course, in alternative embodiments, the housing 2602 may be slightly larger or smaller than that shown. For example, in different embodiments, the housing 2602 may have an internal volume of less than five hundred cubic centimeters, or less than four hundred cubic centimeters, or less than three hundred cubic centimeters, or less than two hundred cubic centimeters, or less than one hundred cubic centimeters, or less than any other volume value that falls between one hundred and five hundred centimeters. In one embodiment, the housing 2602 is sized so that the Pocket Vault 102 may readily fit into the rear pocket of a pair of pants. One feature of the illustrative embodiment of the Pocket Vault 102 shown in

Fig. 2 which may permit its size to be reduced below that of a standard personal computer is the fact that the embodiment shown lacks a disk drive (either hard or floppy) or any similar memory storage device (e.g., a tape drive) that consumes a significant volume within the housing 2602. It should be appreciated, of course, that alternative embodiments may include such memory devices, and that the invention is not necessarily limited to embodiments that exclude them. In addition to the lack of a disk drive or the like, in some embodiments, the power manager 214 may reduce the power consumption of the active components of the Pocket Vault 102 well below that of a standard personal computer, thereby enabling a very small and light weight battery to be employed, as opposed to the relatively large and heavy batteries typically employed in personal computers.

The housing 2602 may provide a water-resistant or waterproof environment for the components housed thereby. The housing materials of Pocket Vaults 102 may be brightly colored, in addition to traditional black or brown, thereby helping their holders to make a fashion statement and/or permitting them to be readily spotted if misplaced. Deluxe versions may be clad in leather, Kevlar™, Gortex™, aluminum and/or stainless steel. In some embodiments, the housing 2602 may even be woven into garments.

Referring again to Fig. 2, any of a number of devices may be used to implement the controller 202, and the invention is not limited to any particular type of controller. In one illustrative embodiment, for example, the controller 202 comprises a low-power multiprocessor or microcomputer having an on-board SRAM and/or flash memory and a real time clock calendar. One example of a suitable controller is the "Motorola Dragonball" Processor from Motorola, Inc. (www.motorola.com). The controller 202 may include a software-programmable and encryption-protected or hard-wired unique chip ID. In one embodiment, this chip ID is released from the Pocket Vault 102 only after the fingerprint scanner 220 (discussed below) has successfully authenticated the identity of the holder. A signal processor for Bluetooth or another wireless connection may also be employed within or along with the controller 202.

The transceiver 204 may be any type of transceiver (or separate transmitter and receiver) capable of communicating with the other devices in the network 100 to enable the functionality described herein. For example, either an RF or an IR transceiver may be employed. Some embodiments may, in fact, include both an IR and an RF transceiver to be used in different applications. For example, an IR transceiver may be employed to interface

the Pocket Vault with a "docking station" type interface unit, and a separate RF transceiver may be employed to communicate over a wireless network such as Bluetooth.

In one illustrative embodiment, the user input device 206 is implemented as part of a touch-screen display used as the display 216 (described below). Additionally or alternatively, the user input device 206 may include dedicated buttons, a keypad, a touch pad, a microphone and speech recognition software, a wand or joystick, or any other suitable implement that permits a person to provide input to the controller 202. The user input device 206 may also be integrated into the fingerprint scanner 220 or into an alternative bio-metric input device. By manipulating the user input device 206, a Pocket Vault holder may select one of a number of media stored in memory of the Pocket Vault 102 for display and/or use in connection with a transaction, and may otherwise control or provide input to software executing on the controller 202. In one embodiment, a keypad is employed as the user input device 206, thereby permitting the holder to input a PIN code as a means of authenticating the holder's identity.

The docking interface 208 may take on any of numerous forms, and the invention is not limited to any particular type of interface device. The docking interface 208 may, for example, include a multi-pin plug adapted to mate with a receptacle disposed on the interface units 104a-c, or vice versa. The docking interface 208 may also comprise one or more implements (e.g., grooves or keys) to ensure that the plug or other docking interface 208 mates correctly with the reciprocal device on an interface unit 104 when the two are physically mated together.

The read/write memory 210 may take on any of a number of forms, and the invention is not limited to any particular type of memory. The memory 210 may, for example, comprise a suitable non-volatile SRAM. Similarly, any suitable memory device that permits a only single write operation to take place may be employed as the write-once memory 212. The memory 210 may have instructions stored therein which, when executed by the controller 202, cause the controller 202 to implement the routines/software described below in connection with Figs. 7-12 and/or Fig. 28. Of course, the memory 210 may also contain a suitable operating system (e.g., Palm OS, Microsoft's Windows CE, Microsoft's Windows for Smartcards, or some similar offering), appropriate device drivers, and other software employed in connection with the controller 202 and/or the peripherals thereof. The memory 210 may also be used to store the various media and personal information retained by the

Pocket Vault 102. In one illustrative embodiment, the memory 210 stores a plurality of different media issued by different and unrelated media issuers, including both financial (e.g., a credit or debit card) and non-financial media (e.g., a drivers license or a library card). Other examples of media or information that may be stored in the memory 210 include: a social security card, identification cards, membership cards, discount cards, commuter passes, toll passes, transit cards, access tools such as hotel keys, business cards, coupons, concert and theatre tickets, transportation tickets, frequent customer cards (e.g., a frequent flier card), medical information cards, receipt information, photographs, etc.

As used herein, "financial media" refers to any media which can, as a matter of course, be used to purchase goods or services, whereas "non-financial media" refers to any media which, while possibly having some value to the Pocket Vault holder, cannot, as a matter of course, be used to purchase goods or services. Examples of financial media include value-linked and value-based media such as debit or credit cards issued by a bank or other financial institution, telephone calling cards, etc. Examples of non-financial media include: library cards, driver's licenses, building access cards, etc. In one embodiment, the memory 210 is large enough to store as many as one hundred compressed graphic image files, and full data sets for as many as one hundred types of media.

In addition, the memory 210 may store status information, where useful, for each type of media. Examples of this sort of status information include: information regarding the value remaining on a pre-paid phone card, information regarding an accumulated number of frequent flier miles, information regarding a total number of cups of coffee that have been purchased at a particular coffee shop (e.g., in connection with a buy-ten-get-one-free special), etc. The portion of the memory 210 devoted to memory storage may be divided into three sections: (1) a high-security section, (2) a medium security section, and (3) a non-secure section. The high security section may be used to store value-based or value-linked media such as debit and credit cards and certain ID information such as driver's licenses, passports, building security passes, etc. The medium security section may be used to store low-value, limited use media that may be accessed, for example, by retailers to keep track of frequent purchase credits or the like. The non-secure section may, for example, be used to store notes, membership ID records, emergency contact information, etc. Access to the information included in the various sections may require security or user authentication procedures commensurate with the indicated security level. For example, an accurate fingerprint scan

and an accurate pin code entry may be required to access the high-security section, only an accurate PIN code entry (even by the retailer) may be required to access the medium-security section, and anyone may be permitted to access the non-secure section.

The power manager 214 may comprise any of numerous devices, and the invention is not limited to any particular type of power supply/management device. The power manager may, for example, employ a flat, rechargeable, lithium battery, and associated regulator and power management software. Alternatively, the battery used may be non-rechargeable and/or coin cell-shaped. Solar powered cells may also be a viable option as at least a supplement to battery power, if not a primary source of power for the Pocket Vault 102. This may be made possible because of the typically modest on-time requirements for a Pocket Vault 102. Power management software may also assist in minimizing the power consumption of the Pocket Vault 102. Such software may, for example, invoke an auto-shutdown feature after a preference-set number of seconds, may control the level of screen back-lighting in response to feedback received from a photo-sensor that registers ambient light, and/or may provide battery charge level warnings to Pocket Vault holders.

The indicator 215 may be any device capable of generating a perceptible indication to the holder such as a bell, chime, buzzer, light, vibration, etc., and the invention is not limited to any particular type of device for accomplishing such a result. In one embodiment, for example, the indicator is a chime generator that generates a "chime" sound that can be heard by the Pocket Vault holder.

Any of a number of devices may also be used for the display 216, and the invention is not limited to any particular type of display. As mentioned above, in one embodiment, a touch-screen display may be employed such that at least a portion of the functionality of the user input device 206 may be incorporated therein. Suitable displays may, for example, include any of a black & white, gray-scaled, or color LCD display, or an LCD bi-stable display.

As mentioned above, the use of the display 216, together with the user input device 206 (which may constitute the touch-screen functionality of the display 216) permits the Pocket Vault holder to flip or scroll through the various media stored in the memory 210 in much the same way as a person flips through the contents of his or her wallet. As mentioned above in connection with the description of the indicator 215, in addition to or in lieu of the display 216, other user output devices may also be employed to provide information to the

Pocket Vault holder. For example, light emitting diodes (LEDs), a beeper or buzzer, a speech synthesizer, a vibrator, etc., may be employed in some embodiments of the Pocket Vault 102.

The token port 218 of the Pocket Vault 102 may comprise a cavity or slot in which the token 102a is retained until it is released to be used to engage in a transaction, as well as the hardware employed to secure the token 102a in place when the token 102a has not been authorized to be released. In one embodiment, the token 102a stores a unique (and possibly encrypted) chip ID which is accessible to another device only when the token 102a is successfully released form the token port 218. In addition to the elements described above, the card port 218 may include additional hardware employed in connection with properly generating or configuring the token 102a prior to its release. This hardware is discussed in more detail below in connection with Fig. 6.

The fingerprint scanner 220 may comprise any device capable of accurately scanning a fingerprint of an individual for comparison with one or more fingerprint images stored in memory. The fingerprint scanner 220 may, for example, be a solid-state (non-optical) device. Devices that may be suitable for use as the fingerprint scanner 220 are available, for example, from Veridicom, Inc., of Santa Clara, California (www.veridicom.com), from Polaroid Corporation of Cambridge, Massachusetts (www.polaroid.com), and from Identix Incorporated of Sunnyvale, California (www.identix.com). The fingerprint scanner 220 may incorporate a temperature sensor that enables it to ensure that a live finger is contacting the scanning surface when the scanning function is employed. In addition to or in lieu of a fingerprint scanner, other bio-metric scanning devices may also be employed to verify the identity of the holder. For example, some embodiments may employ a charge coupled device (CCD) to serve as an iris or retina scanner, an optical sensor, and/or a voiceprint. Alternatively or additionally, a keystroke rhythm may be measured, either alone or in combination with another user authentication technique (e.g., a successful PIN code entry requirement), to validate the identity of the holder. The fingerprint scanner 220 and/or other bio-metric scanners may have touch pad capabilities built into them, thereby permitting them to constitute at least a part of the user input device 206 shown in Fig. 2.

Fig. 3 is a block diagram showing an example embodiment of one of the interface stations 104a-c shown in Fig. 1. The hardware employed to implement each of the stations 104a-c may be identical to the others or may be substantially different, depending on the environment in which the station 104 is to be used, as well as the functional requirements of

the particular station. Therefore, while the example embodiment described herein may be suitable for use as any of the stations, it should be appreciated that each of the stations may, in fact, be configured quite differently than the others.

As shown in Fig. 3, each interface station 104 may include both an the interface station computer 304 and a pocket vault interface unit 302. The interface station computer 304, for example, may be a standard desktop personal computer (PC), and may, as shown, comprise a controller 308, a user input device 318, a memory 320, a modem 322, and a display 324. These components are well known in the art and therefore will not be described in detail herein. The memory 320 of the interface station computer 304 may have instructions stored therein which, when executed by the controller 308, cause the controller to implement the routine described below in connection with Figs. 14-18 as well as any other software, e.g., a browser, drivers, etc., executing on the interface station computer 304.

The pocket vault interface unit 302 is coupled to the interface station computer 304 such that a controller 306 of the pocket vault interface unit 302 can communicate with the controller 308 of the interface station computer 304. The communications interface between these devices may, for example, comprise a Smartcard, Bluetooth or USB interface. As shown, in addition to the controller 306, the pocket vault interface unit 302 may comprise a transceiver 310, a docking interface 312, a finger print scanner 316, a stripe reader 315, and a memory 314. Further, although not shown in Fig. 3, the pocket vault interface unit 302 may also comprise a display and/or another device used to provide feedback to the operator, e.g., an audio indicator or LED.

The stripe reader 315 may be any conventional device for electronically reading the magnetic stripe on a token card such as a credit/debit card or drivers license. The stripe reader 315 may be used, for example, to read information from a token card so that such information can be downloaded to the network server 114 or the Pocket Vault 102.

The memory 314 may be any conventional memory suitable to store the software executed by the controller 306, as well as any data, e.g., stored fingerprint data, used in connection therewith. For example, the memory 314 of the pocket vault interface unit 302 may have instructions stored therein which, when executed by the controller 306, cause the controller 306 to implement the routine described below in connection with Fig. 13.

As with the transceiver 204 of the Pocket Vault 102, the transceiver 310 of the pocket vault interface unit 302 may be any type of transceiver (or separate transmitter and receiver)

capable of communicating with the other devices in the network 100 to enable the functionality described herein. For example, either an RF or an IR transceiver may be employed. Some embodiments may even include both an IR and an RF transceiver to be used in different applications. For example, an IR transceiver may be employed to interface the pocket vault interface unit 302 with a Pocket Vault 102, and a separate RF transceiver may be employed to communicate over a wireless network such as Bluetooth.

As with the docking interface 208 of the Pocket Vault 102, the docking interface 312 of the pocket vault interface unit 302 may take on any of numerous forms, and the invention is not limited to any particular type of interface device. The docking interface 312 may, for example, include a multi-pin plug adapted to mate with a receptacle used as the docking interface 208 of a Pocket Vault 102, or vice versa. The docking interface 312 may also comprise one or more implements (e.g., keys or grooves) to ensure that the plug or the like of the docking interface 208 of the Pocket Vault 102 mates correctly with the corresponding implement of the docking interface 312 when the Pocket Vault 102 and pocket vault interface unit 302 are physically mated together.

Finally, as with the fingerprint scanner 220 of the Pocket Vault 102, the fingerprint scanner 316 of the pocket vault interface unit 302 may comprise any device capable of accurately scanning a fingerprint of an individual for comparison with one or more fingerprint images stored in memory. The fingerprint scanner 316 may, for example, be a solid-state (non-optical) device. Devices that may be suitable for use as the fingerprint scanner 220 are available, for example, from Veridicom, Inc., of Santa Clara, California (www.veridicom.com), from Polaroid Corporation of Cambridge, Massachusetts (www.polaroid.com), and by Identix Incorporated of Sunnyvale, California (www.identix.com). The fingerprint scanner may incorporate a temperature sensor that enables it to ensure that a live finger is contacting the scanning surface when the scanning function is performed. In addition to or in lieu of a fingerprint scanner, other bio-metric scanning devices may also be employed to verify the identity of the interface station operator. For example, some embodiments may employ a charge coupled device (CCD) to serve as an iris or retina scanner, an optical sensor, and/or a voiceprint. Alternatively or additionally, a keystroke rhythm may be measured, either alone or in combination with another user authentication technique (e.g., a successful PIN code entry requirement), to validate the identity of the operator. Although not shown, the pocket vault interface unit 302 may

additionally comprise one or more user input devices enabling the operator to control or provide input to the pocket vault interface unit 302 or the software executing thereon. The fingerprint scanner 316 and/or other bio-metric scanners may, for example, have touch pad capability capabilities built into them, thereby permitting them to constitute such a user input device. Separate user input devices may also be employed.

Fig. 4 shows an example embodiment of the network server 114 shown in Fig. 1. As shown, the network server 114 may comprise one or more controllers 402, as well as a local memory 404, a database 406, and a transceiver 408 coupled thereto. The illustrated components of the network server 114 are well known, and therefore will not be described in detail. The transceiver 408 may, for example, be used to communicate with other devices in the network system 100 (Fig. 1) using a wireless network such as Bluetooth. The controller 404 may also communicate with other network devices via the Internet or a direct connection such as the type established using a dial up modem.

The local memory 404 may have instructions stored therein which, when executed by the controller 402, cause the controller 402 to implement the routines described below in connection with Figs. 19-25 and/or Figs. 30-39. In some embodiments, the local memory 404 and/or database 406 act as a website and execute software which may be accessed by a browser or similar software module operating on a computer. One such embodiment is described below in connection with Figs. 28-39.

The database 406 may, for example, comprise a relational database, and may be used to store the majority, if not all, of the data maintained by the network server 114. The database 406 may, for example, keep a real-time record of critical reference data along with transaction histories, back-up files, and security audit trail information for key events. Examples of specific items that may be stored in the database 406 include: a list of current Pocket Vault holders and appropriate contact information for each; records regarding the versions of software loaded onto each Pocket Vault 102, each pocket vault interface unit 302, and each interface station computer 304; a list of currently authorized or registered Pocket Vaults 102, identified by chip ID and linked to the holder list; a list of currently authorized or registered tokens 102a, identified by chip ID and linked to the holder list; a list of currently authorized locations for interface stations 104 and telephone or other access lines therefor, including business information for each such location and an indication as to the type of interface station 104 it is (e.g., a validation interface station, a personal interface station, or a

commercial interface station); a list of currently authorized or registered interface station operators and the interface stations 104 with which they are associated; a list of currently authorized or registered interface stations 104, identified by chip ID and linked to the list of authorized operators therefor, as well as encrypted cookie ID information (if any) for the respective interface stations 104; authorized media data received from media issuers that has not yet been downloaded to individual Pocket Vaults 102; backup data sets for individual Pocket Vault holders; detailed transaction histories for Pocket Vault registrations indicating where each Pocket Vault 102 was shipped from and to, where each Pocket Vault 102 was registered, which authorized interface station operator conducted the registration process, when that authorized operator was added to the list of authorized operators at a particular location, who submitted the key information to add the operator, which corporate representative associated with the network server 114 met with which representative associated with the interface station in establishing each new location for a validation interface station 104a, to whom and when each Pocket Vault 102 was issued; and communication encryption protocols. Each Pocket Vault account defined on the network server 114 may be defined to support multiple Pocket Vaults 102, as well as to identify other family members who may share certain contents of the Pocket Vaults 102 (e.g., family membership in a local museum).

The network server 114 may analyze data regarding consumer transactions, and thereby accumulate demographic information. Using this information, merchants, media issuers, and/or advertisers may, for example, define targeted marketing programs, which the network server 114 may then deliver to Pocket Vault holders that meet particular demographic profiles.

Fig. 5 shows how the memory 210 of the Pocket Vault 102 (Fig. 2) may be organized (conceptually) in accordance with one embodiment of the invention. The purpose of each of the illustrated memory components will be readily understood by those skilled in the art of the invention, and therefore will not be explained in detail.

Fig. 6 is a block diagram showing an example embodiment of the token 102a shown in Figs. 1 and 2. As shown, the token 102 may be equipped with a controller 602. In the embodiment shown, the controller 602 may be selectively programmed, for example, via interface terminals 606 to generate a current in a wire loop 608 so as to generate a magnetic field about the wire loop 608 that simulates a magnetic stripe of a standard credit card-like

token. In other words, a magnetic field may be generated along the edge of the token 102a as if a magnetic stripe were present on that edge. The location of the simulated magnetic stripe on the token 102a is identified in Fig. 6 as a virtual magnetic stripe 610.

Appropriate software may be loaded onto the controller 602 (e.g., in an on-board memory of the controller 602) so as to enable the controller to generate the virtual magnetic stripe 610. When the token 102a is disposed in the token port 218, the terminals 606 of the token 102a may engage corresponding terminals of the token port 218, thereby enabling the controller 602 to be programmed appropriately. The programming of the controller 602 may be effected, for example, in response to commands from the controller 202 of the Pocket Vault 102, which commands may be generated in response to software executing on the controller 202.

As shown, the controller 602 may be powered by an appropriate resistor-capacitor (RC) circuit which stores a charge that decays over time. The RC circuit may be initially charged via the terminals 606 when the token 102a is disposed in the token port 218 and the controller 602 is being programmed. After the token 102a is removed from the token port 218, the controller 602 will remain powered only so long as sufficient charge remains stored by the RC circuit 604. Because the controller 602 can generate the virtual magnetic stripe 610 only when it is driven by an adequate power supply, the virtual magnetic stripe will disappear after the charge in the RC circuit 604 has decayed beyond a certain threshold level. Because the decay of an RC circuit is reasonably predictable, the virtual magnetic stripe 610 is disposed on the token 102a only for a finite, predetermined period of time after the token 102a is removed from the token port 218. In one embodiment, after the controller 602 loses power, the information with which it was programmed to enable it to generate the virtual magnetic stripe 610 is also lost. Therefore, the virtual magnetic stripe 610 of the token 102a cannot be used again until the controller 602 is again powered up and reprogrammed. Alternatively, the controller 602 may cut off the power to the wire loop 608 after a preset amount of time or an amount of time determined by the Pocket Vault holder (possibly within preset limits). Additionally or alternatively, the token 102a may have its own embedded chip ID, which may be accessible only when the token 102a is successfully released form the token port 218.

In some embodiments, the token 102a may possess the characteristics of a bank-issued Smartcard, either in addition to or in lieu of the virtual magnetic stripe 610.

Accordingly, the token 102a may include a specialized Smartcard chip or the controller 602 may be programmed to mimic such a chip. In any event, the token 102a may be preloaded with the bank's chip operating system (OS) and possibly customer-specific secure information. In such embodiments, the functionality of the Smartcard components may, for example, be enabled only in response to successful authentication of the Pocket Vault holder, e.g., using the fingerprint scanner 220 of the Pocket Vault 102. Therefore, the customer-specific "Smartcard" information may remain inaccessible so long as the Pocket Vault holder's identity has not been authenticated using the Pocket Vault 102.

As mentioned above, Figs. 7-12 are flow diagrams illustrating an example implementation of software that may be executed by the controller 202 of the Pocket Vault 102. As described below, this or additional proprietary software may enable menu structures, handle preference management, provide the data on and safeguard the programmability of the virtual magnetic stripe 610 (if so equipped), and ensure proper encryption data management. In one embodiment, local software for each Pocket Vault 102 and pocket vault interface station 104 may be upgraded from time to time by automatic download from the network server 114.

During execution of the routines of Figs. 7-12, various items may be displayed on the display 216, including prompts or icons regarding user input options (when a touch-screen display is employed as the display 216 or a point and click mechanism is employed herewith), and various items may also be displayed on the token 102a when the token 102a is ejected from the token port 218 of the Pocket Vault 102. Figs. 26A-P show examples of how the display 216 and the token 102a may appear as the routines of Figs. 7-12 are executed, and therefore will be discussed in connection with the description of these routines.

Fig. 7 is a flow diagram illustrating an example implementation of a primary routine 700 that may be executed by the controller 202 of the Pocket Vault 102. Instructions for the routine 700 may be stored, for example, in the "applications" section 508 of the memory 210 of the Pocket Vault 102.

As shown, the routine 700 begins at a step 702, wherein it is determined whether the Pocket Vault holder has applied his/her fingerprint to the fingerprint scanner 220 of the Pocket Vault 102. At the step 702, the display 216 of the Pocket Vault 102 may appear as shown in Fig. 26A. That is, the display 216 may be blank at the step 702, as the Pocket Vault 102 is currently powered down.

When, at the step 702, it is determined that the holder has applied his/her fingerprint to the fingerprint scanner 220, the routine 700 proceeds to a step 704, wherein the power manager 214 powers on the Pocket Vault 102. The routine 700 otherwise waits at the step 702 until the Pocket Vault holder has applied a fingerprint to the fingerprint scanner 220. Is should be appreciated, however, that, in some embodiments, the step 702 may not represent an instruction set executed by the processor 202. Instead, the step 702 may represent the detection of the occurrence of a physical action, e.g., the activation of a hardware switch, and the power manager 214 may be activated in response to the detection of such an action, without requiring intervention by the processor 202.

After the step 704, the routine 700 proceeds to a step 706, wherein the fingerprint scanner 220 scans the applied fingerprint of the Pocket Vault holder.

After the step 706, the routine 700 proceeds to a step 708, wherein it is determined whether the Pocket Vault 102 has been validated. In one embodiment, the Pocket Vault 102 is not validated until: (1) a user's fingerprints have been stored in the fingerprint memory (e.g., the write-once memory 212 of Fig. 2), and (2) the Pocket Vault 102 has received and stored encrypted validation information (e.g., a PKI certificate) from the network server 114, as described below.

When, at the step 708, it is determined that the Pocket Vault 102 has not yet been validated, the routine 700 proceeds to a step 710, wherein a PROCESS POCKET VAULT VALIDATION routine (described below in connection with Fig. 8) is executed.

When, at the step 708, it is determined that the Pocket Vault 102 has already been validated, the routine 700 proceeds to a step 712, wherein it is determined whether Pocket Vault 102 has been authenticated, e.g., whether the fingerprint scanned at the step 706 matches one of the fingerprints stored in the fingerprint memory 212.

When, at the step 712, it is determined that the Pocket Vault has not been properly authenticated, the routine 700 proceeds to a step 714, wherein an UNAUTHORIZED HOLDER routine (discussed below in connection with Fig. 9) is executed. Figs. 26B-D show how the display 216 of the Pocket Vault 102 may appear during the UNAUTHORIZED HOLDER routine, and therefore are also discussed below in connection with Fig. 9.

When, at the step 712, it is determined that the Pocket Vault 102 has been properly authenticated, the routine 700 proceeds to a step 713, wherein an encrypted message including the unique Pocket Vault chip ID is transmitted to the pocket vault interface unit

302, in the event that the Pocket Vault 102 is interfaced or in communication with such a device.

In some embodiments, before a Pocket Vault holder is granted access to the contents of his or her Pocket Vault 102, a check may be made to ensure that the components used to interface the Pocket Vault 102 with the other components in the network 100 (either wirelessly or directly) are in place and operating correctly, and have not been compromised. Alternatively, the operability and integrity of such components may be checked just prior to their use.

Moreover, in some embodiments, prior to granting a holder access to the contents of the Pocket Vault 102, a check may be made to ensure that the contents of the Pocket Vault 102 have been updated recently. For example, the Pocket Vault 102 may forbid its holder from accessing its contents if the Pocket Vault 102 has not been updated at least 48 hours (or some other specified time period) prior to the attempted use. Updating of the Pocket Vault 102 may be accomplished, for example, using the synchronization or backup and recovery methods described herein.

After the step 713, the routine 700 proceeds to a step 716, wherein it is determined whether the Chameleon Card (i.e., the token 102a) is presently on-board the Pocket Vault 102 (i.e., whether the token 102a is disposed within the card port 218 of Fig. 2).

When, at the step 716, it is determined that the token 102a is not on-board the Pocket Vault 102, the routine 700 proceeds to a step 718, wherein the Pocket Vault holder is informed that the Chameleon Card is not on board, and is asked whether he/she wants to engage in a non-card transaction (i.e., a transaction not involving the token 102a).

After the step 718, the routine 700 proceeds to a step 720, wherein it is determined whether the holder has selected to engage in a non-card transaction.

When, at the step 720, it is determined that the holder has selected not to engage in a non-card transaction, routine 700 returns to the step 716 (described above), wherein it is again determined whether the Chameleon Card is on board the Pocket Vault 102. Therefore, the holder is permitted to engage in a transaction involving the Chameleon Card only when it has been confirmed that the Chameleon Card is on board the Pocket Vault 102.

When, at the step 720, it is determined that the holder has selected to engage in a non-card transaction, the routine 700 proceeds to the step 722, wherein the AUTHORIZED HOLDER routine (discussed below in connection with Figs. 10 and 11) is executed.

When, at the step 716, it is determined that the Chameleon Card is on-board the Pocket Vault 102, the routine 700 also proceeds to the step 722, wherein the AUTHORIZED HOLDER routine (discussed below in connection with Figs. 10 and 11) is executed. Figs. 26G-N and 26P show how the display 216 of the Pocket Vault 102 and the token 102a ejected therefrom may appear (when employed) during the AUTHORIZED HOLDER routine, and therefore are also discussed below in connection with Figs. 10 and 11.

After each of the steps 710, 714, and 720 (only one of which is executed during each iteration of the routine 700), the routine 700 proceeds to a step 724, wherein the VERIFY CARD RETURN routine (discussed below in connection with Fig. 12) is executed. Fig. 26O shows how the display 216 of the Pocket Vault 102 may appear during the VERIFY CARD RETURN routine, and therefore is also discussed below in connection with Fig. 12.

After the step 724, the routine 700 proceeds to a step 726, wherein the screen of the display 216 is caused to flash to indicate that the Pocket Vault 102 is being shut down.

After the step 726, the routine 700 proceeds to a step 728, wherein the Pocket Vault 102 is powered down.

After the step 728, the routine 700 returns to the step 702, wherein the Pocket Vault 102 again waits for a fingerprint to be applied to the fingerprint scanner 220, and wherein the display 216 may again appear as shown in Fig. 26A.

Fig. 8 is a flow diagram illustrating an example embodiment of the PROCESS POCKET VAULT VALIDATION routine shown in Fig. 7 (step 710).

As shown, the routine 710 begins at a step 801, wherein the holder is informed (e.g., on the display 216) that the Pocket Vault 102 is not currently validated, and that the holder must interface the Pocket Vault 102 with an interface unit 302 of an appropriate interface station 104 (e.g., a validation interface station 104a) if the holder desires to validate the Pocket Vault 102.

After the step 801, the routine 710 proceeds to step 802, wherein it is determined whether the Pocket Vault 102 has been interfaced with an appropriate interface unit 302.

When, at the step 802, it is determined that the pocket vault 102 has not yet been interfaced with an appropriate interface unit 302, the routine 710 returns to the step 801 (discussed above).

When, at the step 802, it is determined that the Pocket Vault 102 has been interfaced with an appropriate interface unit 302, the routine 710 proceeds to a step 803, wherein it is determined whether the fingerprint memory, e.g., the write-once memory 212, is empty.

When, at the step 803, it is determined that the fingerprint memory is empty, the routine 710 proceeds to a step 804a, wherein the holder is prompted to apply a fingerprint from one finger of his or her left hand to the fingerprint scanner 220, waiting for a "beep" to be emitted (e.g., by indicator 215) after each fingerprint application.

Next, during steps 806a – 810a, the routine proceeds until the fingerprint of the selected finger has been scanned three times successfully.

After the steps 806a-810a, the routine proceeds to a step 804b, wherein the holder is prompted to apply a fingerprint from one finger of his or her right hand to the fingerprint scanner 220, waiting for a "beep" to be emitted (e.g., by indicator 215) after each fingerprint application.

Next, during steps 806b – 810b, the routine proceeds until the fingerprint of the selected finger has been scanned three times successfully.

After completing the steps 806b-810b, when a total of six fingerprints have been stored in memory, the routine 710 proceeds to a step 812, wherein an encrypted message including the pocket vault ID is transmitted to the interface unit 302, for ultimate transmission to the network server 114.

When, at the step 803, it is determined that the fingerprint memory, e.g., the write-once memory 212, is not empty, the routine 710 proceeds to a step 811, wherein it is determined whether the fingerprint scanned at the step 706 (Fig. 7) matches one of the stored fingerprints.

When, at the step 811, it is determined that the fingerprint scanned at the step 706 does match one of the stored fingerprints, the routine 710 proceeds to the step 812 (discussed above).

When, at the step 811, it is determined that the fingerprint scanned at the step 706 does not match any of the stored fingerprints, the routine 710 proceeds to a step 818, wherein an indication (e.g., a message on the display 216 or an audio signal from the indicator 215) is generated to inform the holder that the validation attempt was unsuccessful.

After the step 818, the routine 710 terminates.

After the step 812, the routine 710 waits at steps 814 and 816 to determine whether an encrypted message including validation information (e.g., a PKI certificate) has been received from the interface unit 302. This encrypted validation information may, for example, be received by the Pocket Vault 102 via either the docking interface 208 or the transceiver 204 of the pocket vault interface unit 302 of a validation interface station 104a. As discussed in more detail below, this encrypted validation information may, for example, be generated by the network server 114 and forwarded to the pocket vault interface unit 302 of a validation interface station 104a (via the interface station computer 304 of the validation interface station 104a) after certain conditions have been met. The network server 114 may therefore ultimately determine whether each Pocket Vault 102 is permitted to receive this validation information.

When, at the step 816, it is determined that the time-out period has elapsed, the routine 710 proceeds to the step 818 (discussed above).

When, at the step 814, it is determined that encrypted validation information has been received before the timeout period of the step 816 has elapsed, the routine 710 proceeds to a step 820, wherein the validation information is stored in memory.

After the step 820, the routine 710 proceeds to a step 822, wherein an indication (e.g., a message on the display 216 or an audio signal from the indicator 215 of the Pocket Vault 102) is generated to inform the holder that the Pocket Vault 102 has been successfully validated.

After the step 822, the routine 710 terminates.

Fig. 9 is a flow diagram illustrating an example implementation of the UNAUTHORIZED HOLDER routine shown in Fig. 7 (step 714).

As shown, the routine 714 begins at a step 902, wherein a menu is displayed on the display 216 that permits the holder to select one of several options: (1) TRY AGAIN, (2) POCKET VAULT RETURN INFORMATION, (3) EMERGENCY INFORMATION, or (4) END SESSION. Fig. 26B shows how the display 216 may appear when the step 902 is reached. As shown, textual information and/or icons representing the various menu options may be displayed to the holder.

After the step 902, the routine 714 proceeds to a step 904, wherein the routine 714 waits for one of the displayed menu items to be selected by the holder (e.g., when the holder touches the location on the screen of the display 216 at which the menu item is displayed).

After one of the menu items has been selected at the step 904, the routine 714 proceeds to a step 906, wherein it is determined whether the TRY AGAIN option was selected. By selecting TRY AGAIN, the holder may request that the holder again be permitted to attempt to access the secure contents of the Pocket Vault 102 by reapplying the holder's fingerprint to the fingerprint scanner 220.

When, at the step 906, it is determined that the user has selected the TRY AGAIN option, the routine 714 proceeds to a step 912, wherein it is determined whether this is the third sequential time that the scanned fingerprint has failed to match the fingerprint stored in memory.

When, at the step 912, it is determined that three sequential failed matches have occurred, the routine 714 proceeds to a step 914, wherein certain security precautions are taken in light of the multiple failed attempts to match the holder's fingerprint with that stored in the Pocket Vault 102. For example, when multiple failed matches have occurred, the Pocket Vault's secure memory may be erased, a security alert message may be broadcast by the transceiver 204 and/or any other prudent steps may be taken to ensure that an unauthorized user does not access the Pocket Vault's sensitive contents.

After the step 914, the routine 714 terminates.

When, at the step 912, it is determined that this is not the third consecutive time that the holder's fingerprint has failed to match that stored in the Pocket Vault's memory, the routine 714 terminates, and the holder may then again attempt (at the step 702) to access the Pocket Vault 102 by reapplying his/her fingerprint to the fingerprint scanner 220.

When, at the step 906, it is determined that the TRY AGAIN option has not been selected, the routine 714 proceeds to a step 908, wherein it is determined whether there exist any nested menu items for the menu item selected at the step 904.

When, at the step 908, it is determined that nested menu items do exist for the selected menu item, the routine 714 proceeds to a step 910, wherein the nested menu items for the selected menu item are displayed to the holder on the display 216.

After the step 910, the routine 714 returns to the step 904, wherein the routine 714 again waits for the holder to select one of the displayed menu items.

When, at the step 908, it is determined that no nested menu items exist for the selected menu item, the routine 714 proceeds to a step 916, wherein it is determined whether the END SESSION option has been selected.

When, at the step 916, it is determined that the END SESSION option has been selected, the routine 714 terminates.

When, at the step 916, it is determined that the END SESSION option has not been selected, the routine 714 proceeds to a step 918, wherein the information, if any, for the selected menu item is displayed to the holder on the display 216. Because the step 918 is reached only after a failed attempt to match the holder's fingerprint with that stored in the memory of the Pocket Vault 102, the information displayed at the step 918 may, for example, include information as to where the Pocket Vault 102 may be returned if it is found by someone other than the Pocket Vault holder (see Fig. 26C), or may be emergency information regarding the holder such as the holder's blood type, allergies, persons to contact in case of an emergency, etc. (see Fig. 26D). It should be appreciated that any of a number of non-secure media may be selected using the menu access routine discussed above in connection with steps 904-910, and may be displayed to the person accessing the Pocket Vault 102, regardless of the identity of that person. Of course, this non-secure information may be information that the holder would not mind falling into the hands of a stranger should the holder misplace or have his/her Pocket Vault 102 stolen.

After the step 918, the routine 714 proceeds to a step 920, wherein after a delay of a certain period of time (e.g., thirty seconds), the holder is prompted to reapply his/her fingerprint within a particular period of time (e.g., ten seconds) to avoid shut down of the Pocket Vault 102.

After the step 920, the routine 714 proceeds to a step 922, wherein it is determined whether a fingerprint has been reapplied to the fingerprint scanner 220 within ten seconds.

When, at the step 922, it is determined that a fingerprint has been reapplied to the fingerprint scanner 220 within ten seconds, the routine 714 returns to the step 918 (discussed above), wherein the selected information is again displayed to the user.

When, at the step 922, it is determined that a fingerprint has not been reapplied to the fingerprint scanner 220 within ten seconds, the routine 714 terminates.

Fig. 10 is a flow diagram illustrating an example implementation of the AUTHORIZED HOLDER routine of Fig. 7 (step 722).

As shown, the routine 722 begins at a step 1002, wherein it is determined whether an advertisement is scheduled for display on the Pocket Vault 102. Information regarding whether certain advertisements are to be displayed by the Pocket Vault 102 may have been

uploaded, for example, from the personal interface station 104b in response to the holder previously interfacing the Pocket Vault 102 with the personal interface station 104b to synchronize the contents of the Pocket Vault 102 with information stored on the network server 114. The advertiser 108 (Fig. 1) may, for example, have made arrangements with the company operating the network server 114 to have certain advertising information uploaded to Pocket Vaults 102 when particular Pocket Vault holders interface their Pocket Vaults 102 with their personal interface stations 104b.

When, at the step 1002, it is determined that an advertisement has been scheduled, the routine 722 proceeds to a step 1004, wherein the scheduled advertisement is displayed, for example, for approximately two seconds. Fig. 26I shows an example of how the display 216 may appear when such an advertisement is displayed.

After the step 1004, the routine 722 proceeds to a step 1006, wherein a "welcome screen" is displayed for a brief period (e.g., one second). Fig. 26G shows an example of how the display 216 may appear when such a welcome screen is displayed.

When, at the step 1002, it is determined that an advertisement is not scheduled, the routine 722 proceeds immediately to the step 1006, and no advertisement is displayed to the Pocket Vault holder.

After the step 1006, the routine 722 proceeds to a step 1008, wherein it is determined whether a "preferred" menu has been selected or pre-set for initial display to the Pocket Vault holder.

When, at the step 1008, it is determined that a preferred menu has been selected or pre-set, the routine 722 proceeds to a step 1012, wherein the display 216 fades to the preferred menu. Figs. 26H and 26J show examples of how the display 216 may appear when such a preferred menu is displayed. In the example of Fig. 26H, the preferred menu immediately shows the holder's preferred credit card as the selected menu item. Should the holder opt to use this media to engage in a transaction, the holder can simply choose the media directly. Alternatively, the holder may opt to access the HOME menu or other menu items by selecting appropriate icons displayed on the screen. In the example of Fig. 26J, the preferred menu immediately shows, perhaps, a selected group of the holder's most frequently used menu items.

When, at the step 1008, it is determined that a preferred menu has not been selected or pre-set, the routine 722 proceeds to a step 1010, wherein the display 216 fades to a standard

HOME menu of secure items. Fig. 26L shows an example of how the display 216 may appear when the HOME menu is displayed.

After either one of the steps 1010 and 1012 has been executed, the routine 722 proceeds to a step 1014, wherein the routine 722 waits for the holder to select one of the displayed menu items.

When, at the step 1014, it is determined that the holder has selected a particular menu item, the routine 722 proceeds to a step 1016, wherein it is determined whether the holder has selected to enter or return to the HOME menu.

When, at the step 1016, it is determined that the holder has selected the HOME option, the routine 722 proceeds to the step 1010, wherein the HOME menu of secure items is displayed.

When, at the step 1016, it is determined that the holder has selected a menu item other than the HOME option, the routine 722 proceeds to a step 1018, wherein it is determined whether there exist any nested menu items for the selected menu item.

When, at the step 1018, it is determined that nested menu items do exist for the selected menu item, the routine 722 proceeds to a step 1020, wherein the nested menu items for the selected menu item are displayed. Thus, the holder may work his/her way through various layers of menu items until the desired menu item is reached. It should be appreciated that the menu items on the higher-level layers therefore may be categorized so as to enable the holder to quickly reach the desired media or other menu option.

When, at the step 1018, it is determined that no nested menu items exist for the selected menu item, the routine 722 proceeds to a step 1022, wherein it is determined whether the holder has selected a media from among the available menu items.

When, at the step 1022, it is determined that the holder has not selected a media, the routine 722 proceeds to a step 1040, wherein information relating to the selected non-media item may be displayed, or some other function may performed in accordance with the holder's selection. A non-media menu selection may involve, for example, preference settings for certain functional aspects of the Pocket Vault 102, e.g., whether the holder has a preferred secure menu (see step 1008). Preferences for the services or the device can be selected and, as appropriate, distributed to the Pocket Vault 102 either on the spot or the next time the Pocket Vault 102 is interfaced with an appropriate interface station 104. Preferences may, for example, include definition of home pages, connection of secure and non-secure

media, order of media presentment, sort orders, user interface options, synchronization defaults, etc. Preferences that determine which items are displayed on the home page or on other pages may be defined. For example, a Pocket Vault holder may set up three preference sets: one for "business," one for "personal," and one for "vacation." The "personal" and "business" preference sets may be set to be effective at different times of the day and/or different days of the week. The "vacation" preference set may be made effective for specific blocks of time determined by the Pocket Vault holder, possibly overriding the normal timing of the "personal" and "business" sets. The Pocket Vault holder may choose to establish the various preference settings based on his or her judgment or he or she may choose to allow the network server 114, supported by various databases, knowledge of the Pocket vault holder's various media and goals set by the Pocket Vault holder (e.g., minimize interest cost on credit cards or maximize frequent flyer miles, etc.), to determine optimal media use patterns and resulting media menu contents for a particular Pocket Vault holder. Preferences may also be defined between media that will link them for: (a) affiliate credits (like frequent flyer miles) that may be automatically presented to a merchant and tracked for a holder, (b) available discounts afforded by a membership (like senior citizen or AAA discounts), and/or (c) process improvement purposes (e.g., when information needs to be presented in a certain order to work properly). For example, a linkage preference may facilitate presentation of a discount card before presentation of a payment card when buying groceries.

After the step 1040, the routine 722 proceeds to a step 1042, wherein the holder is prompted either to END the session, or to return to the HOME menu.

After the step 1042, the routine 722 proceeds to a step 1044, wherein it is determined whether the holder has opted to END the session or to return to the HOME menu.

When, at the step 1044, it is determined that the holder has selected to return to the HOME menu, the routine 722 proceeds to the step 1010 (discussed above).

When, at the step 1044, it is determined that the holder has opted to END the session, the routine 722 terminates.

When, at the step 1022, it is determined that the holder has selected a media from the displayed menu items, the routine 722 proceeds to a step 1024, wherein the selected media is displayed to the holder on the display 216. The selected media may, for example, be a particular credit card, in which case the name of the credit card and/or the logo for the credit

card and any preferred advertisement, specials, etc., for the selected media may be displayed to the holder as well.

After the step 1024, the routine 722 proceeds to a step 1026, wherein the holder is prompted to choose to: (1) EJECT the card, (2) to invoke a WIRELESS transaction, or (3) to return to the HOME menu.

After the step 1026, the routine 722 proceeds to a step 1028, wherein it is determined which of these three options has been selected by the holder.

When, at the step 1028, it is determined that the holder has opted to return to the HOME menu, the routine 722 proceeds to the step 1010 (discussed above).

When, at the step 1028, it is determined that the holder has selected the EJECT card option, the routine 722 proceeds to a step 1032, wherein it is determined whether the Chameleon Card is on board the Pocket Vault 102 (i.e., whether the token 102a is disposed in the token port 218).

When, at the step 1032, it is determined that the Chameleon Card is not on board the Pocket Vault 102, the routine 722 proceeds to a step 1034, wherein the holder is informed that the Chameleon Card is not on board the Pocket Vault 102.

After the step 1034, the routine 722 proceeds to the step 1026 (discussed above).

When, at the step 1032, it is determined that the Chameleon Card is on board the Pocket Vault 102, the routine 722 proceeds to a step 1036, wherein the PROCESS CARD TRANSACTION routine (discussed below in connection with Fig. 11) is executed.

After the step 1036, the routine 722 proceeds to a step 1038, wherein the VERIFY CARD RETURN routine (discussed below in connection with Fig. 12) is executed.

After the step 1038, the routine 722 proceeds to the step 1042 (discussed above).

When, at the step 1028, it is determined that the holder has opted to invoke a wireless transaction, the routine 722 proceeds to a step 1030, wherein the wireless transaction involving the selected media is executed. This wireless transaction may be invoked, for example, using the transceiver 204 of the Pocket Vault 102 to communicate with the transceiver 310 (Fig. 3) of a commercial interface station 104c (Fig. 1) over a wireless network, such as Bluetooth. As mentioned above, in embodiments that permit wireless transactions, a check of the wireless components may be made (e.g., verifying that an internal antenna (not shown) is in place and connected, and that related circuitry is not defeated or compromised in any way), prior to granting the holder access to the contents of the Pocket

Vault 102. Alternatively, such a check may be made in response to such a wireless transaction being requested, e.g., at the step 1030.

After the step 1030, the routine 722 proceeds to the step 1042 (discussed above).

Fig. 11 is a flow diagram illustrating an example implementation of the PROCESS CARD TRANSACTION routine of Fig. 10 (step 1036).

As shown, the routine 1036 begins at a step 1102, wherein the Chameleon Card is configured to carry the selected media, and is ejected from the card port 218 (Fig. 2). As discussed above, the token 102a may be configured to carry the selected media in any of a number of ways, and the invention is not limited to any particular type of configuration technique. The card may be configured, for example, by causing it to generate a simulated magnetic stripe for a limited period of time, by causing it to have a bar code disposed on it for a limited period of time, or simply by causing a card number to be visibly disposed on it for a limited period of time. One example of technology that may be employed to cause information to appear temporarily on the token 102a is available from E-ink (www.Eink.com). It should be appreciated, of course, that the card need not be temporarily configured in all embodiments, and may alternatively be configured in a more permanent manner in some embodiments.

After the step 1102, the routine 1036 proceeds to a step 1104, wherein the selected media is grayed out on the display 216 to indicate that the media is currently in use by the Chameleon Card. When the selected media is grayed out, the Pocket Vault's ability to configure another Chameleon Card with the grayed out media may also be disabled. Therefore, in such an embodiment, even if the Pocket Vault holder had an additional Chameleon Card available, the Pocket Vault 102 would be incapable of loading that media onto that Chameleon Card.

After the step 1104, the routine 1036 proceeds to a step 1106, wherein it is determined whether the selected media has stored value associated with it. The selected media may, for example, represent a pre-paid calling card from which value is deducted each time the media is used in a particular transaction, or a frequent flier card to which value (e.g., miles) is added in connection with each airline ticket purchased.

When, at the step 1106, it is determined that the selected media does have stored value associated with it, the routine 1036 proceeds to a step 1108, wherein a "stored value

flag" (discussed below in connection with step 1126 of routine 1036 (Fig. 11) and step 1212 of routine 724 (Fig. 12)) is set to TRUE.

After the step 1108, the routine 1036 proceeds to a step 1110, wherein it is determined whether the holder has set a default option so as to permit the holder to maintain expense records by recording transactions into registers assigned to expense categories.

When, at the step 1106, it is determined that the selected media does not have stored value associated with it, the routine 1036 proceeds immediately to the step 1110.

When, at the step 1110, it is determined that the holder has not opted for the ability to maintain expense records, the routine 1036 terminates.

When, at the step 1110, it is determined that the holder has opted for the ability to maintain expense records, the routine 1036 proceeds to a step 1112, wherein the holder is prompted to decide whether to record the currently-pending transaction.

After the step 1112, the routine 1036 proceeds to a step 1114, wherein it is determined whether the holder has opted to record the pending transaction.

When, at the step 1114, it is determined that the holder has not opted to record the transaction, the routine 1036 terminates.

When, at the step 1114, it is determined that the holder has opted to record the transaction, the routine 1036 proceeds to a step 1116, wherein a menu including a number of options involving expense categories are displayed to the holder on the display 216.

After the step 1116, the routine 1036 proceeds to a step 1118, wherein the routine 1036 waits for the holder to select one of the displayed menu options.

When, at the step 1118, it is determined that the holder has selected a menu item, the routine 1036 proceeds to a step 1120, wherein it is determined whether the holder selected the SKIP RECORD option, e.g., when the holder has changed his or her mind and opted not to record a particular transaction.

When, at the step 1120, it is determined that the holder has selected the SKIP RECORD option, the routine 1036 terminates.

When, at the step 1120, it is determined that holder has not selected the SKIP RECORD option, the routine 1036 proceeds to a step 1122, wherein it is determined whether any nested menu items exist for the selected menu item.

When, at the step 1122, it is determined that nested menu items do exist for the selected menu item, the routine 1036 proceeds to a step 1124, wherein the nested menu items are displayed to the holder on the display 216.

After the step 1124, the routine 1036 returns to the step 1118 (discussed above).

When, at the step 1122, it is determined that no nested menu items exist for the selected menu item, the routine 1036 proceeds to a step 1126, wherein it is determined whether the stored value flag was set to TRUE at the step 1108 (discussed above).

When, at the step 1126, it is determined that the stored value flag is set to TRUE, the routine 1036 proceeds to a step 1128, wherein a "record stored value transaction" flag (discussed below in connection with step 1216 of routine 724 (Fig. 12)) is set to TRUE.

After the step 1128, the routine 1036 terminates.

When, at the step 1126, it is determined that the "stored value" flag is not TRUE, the routine 1036 proceeds to a step 1130, wherein the holder is prompted to enter a dollar amount to be recorded for the transaction.

After the step 1130, the routine 1036 proceeds to a step 1132, wherein the routine 1036 waits for the holder to enter a transaction amount. After the holder has entered a transaction amount, the routine 1036 proceeds to a step 1134, wherein a "transaction summary approval" menu is displayed to the holder on the display 216. In the example shown, this menu permits the holder to select (1) to APPROVE the recordation, (2) to change the expense CATEGORY for the transaction, or (3) to change the AMOUNT to be recorded.

After the step 1134, the routine 1036 proceeds to a step 1136, wherein it is determined which of the menu items displayed in step 1134 the holder has selected.

When, at the step 1136, it is determined that the holder has selected to change the transaction AMOUNT, the routine 1036 returns to the step 1130 (discussed above).

When, at the step 1136, it is determined that the holder has opted to change the expense CATEGORY, the routine 1036 returns to the step 1116 (discussed above).

When, at the step 1132, it is determined that the holder has opted to APPROVE the recordation, the routine 1036 proceeds to a step 1138, wherein the entered transaction amount is added to the expense register for the selected category, and the balances associated therewith are updated accordingly.

After the step 1138, the routine 1036 terminates.

Fig. 12 is a flow diagram illustrating the VERIFY CARD RETURN routine of Fig. 7 (step 724).

As shown, the routine 724 begins at a step 1202, wherein it is determined whether the Chameleon Card is currently on board the Pocket Vault 102 (i.e., whether the token 102a is disposed within the token port 218).

When, at the step 1202, it is determined that the Chameleon Card is not on board the Pocket Vault 102, the routine 724 proceeds to a step 1204, wherein the holder is prompted to return the Chameleon Card to the token port 218 (see Fig. 260).

After the step 1204, the routine 724 proceeds to a step 1206, wherein it is determined whether a timeout period (e.g., ten seconds) has elapsed since the user was last prompted to return the Chameleon Card to the token port 218.

When, at the step 1206, it is determined that the timeout period has not yet elapsed, the routine 724 returns to the step 1202 (discussed above).

When, at the step 1206, it is determined that the timeout period has elapsed, the routine 724 proceeds to a step 1208, wherein the user is again prompted to return the Chameleon Card, this time with an audio indication (e.g., a "chime" sound generated by the indicator 215 of Fig. 2).

After the step 1208, the routine 724 proceeds to a step 1210, wherein it is determined whether an extended timeout period (e.g., 10 minutes) has elapsed since the user was first prompted to return the Chameleon Card to the token port 218.

When, at the step 1210, it is determined that the extended timeout period has not yet elapsed, the routine 724 returns to the step 1202 (discussed above).

When, at the step 1210, it is determined that the extended timeout period has elapsed, the routine 724 terminates.

When, at the step 1202, it is determined that the Chameleon Card is on board the Pocket Vault 102 (i.e., the token 102a is disposed within the token port 218), the routine 724 proceeds to a step 1212, wherein it is determined whether the "stored value" flag was set to TRUE in step 1108 of the routine 1036 (Fig. 11).

When, at the step 1212, it is determined that the "stored value" flag is not TRUE, the routine 724 terminates.

When, at the step 1212, it is determined that the "stored value" flag is TRUE, the routine 724 proceeds to a step 1214, wherein the stored value for the selected media is updated based on the amount deducted from the Chameleon Card during its use.

After the step 1214, the routine 724 proceeds to a step 1216, wherein it is determined whether the "record stored value transaction" flag was set to TRUE in the step 1128 of the routine 1036 (Fig. 11).

When, at the step 1216, it is determined that the "record stored value transaction" flag is FALSE, the routine 724 proceeds to a step 1222, wherein the "stored value" flag is set to FALSE.

When, at the step 1216, it is determined that the "record stored value transaction" flag is TRUE, the routine 724 proceeds to a step 1218, wherein the dollar amount of the transaction is added to the selected expense register (i.e., the expense register selected at the step 1118 of the routine 1036 (Fig. 11)). The dollar amount entered is determined based on the dollar amount that was deducted from the stored value on the Chameleon Card as a result of the transaction.

After the step 1218, the routine 724 proceeds to a step 1220, wherein the "record stored value transaction" flag is set to FALSE.

After the step 1220, the routine 724 proceeds to the step 1222 (discussed above)

After the step 1222, the routine 724 terminates.

In addition to a routine such as that discussed above in connection with Figs. 7-12, certain software enhancements may also be disposed in the memory 210 of a Pocket Vault 102 for use with the controller 202. One such software enhancement involves the use of "system preference file" software. This software may establish certain preferences that cannot be altered on the Pocket Vault 102 by the holder, and which may be stored in encrypted form, along with certain information regarding value-based media. For example, Pocket Vaults 102 may be sold with a choice of two or three advertising profiles. During the Pocket Vault registration and validation process (described below), an encrypted system preference file may be created that indicates whether the device was, for example, subject to a "Premium," "Plus" or "Base" profile status. This status may have been selected, for example, on the Pocket Vault 102 itself, or using one of the interface stations 104a-c when the Pocket Vault 102 was interfaced therewith.

Under the "Premium" profile, the Pocket Vault 102 may be advertising-free, but cost a significant amount. Under the "Plus" profile, the Pocket Vault 102 may display only advertising related to shops or services you currently patronize, but cost significantly less than the "Premium" version. Under the "Base" profile, the Pocket Vault 102 may have a variety of advertising on a regular basis, subject only to network "saturation effectiveness" limitations, and the Pocket Vault 102 may be free, or nearly so (e.g., a small purchase charge to generate in-store revenue for the retailer may be charged).

A holder's choice about participation in specific promotional campaigns linked to the holder's buying behavior may also be part of the registration process and affect retail pricing. Once chosen, the network server 114 may send a message to the Pocket Vault 102, e.g., via the validation interface station 104a, and direct the storage of necessary encrypted information on the Pocket Vault 102 (e.g., "Buyer Profile Participant").

The advertising and marketing choices may be changed at a date after purchase and result in a changed set of costs (either credits or debits) to the Pocket Vault holder. Other system preference data may include the "saturation effectiveness" limitations on the amount of advertising that can appear during any given single use window (a particular period during which the device is powered on), any given hour, any given day and/or any given month. The limitations may control both the number of advertisements permitted and the amounts of advertisement time permissible (e.g., seconds per advertisement), by category (e.g., such limitations may, for example, based on categories of advertisements be imposed general advertising, advertising from retailers that the Pocket Vault holder already patronizes and advisory notices from the network server 114. For example, these limits may be set to balance the need for advertising revenue with the need to not overwhelm or annoy Pocket Vault holders. This preference file may, for example, limit all advertising to one advertisement per "on-session," two advertisements per hour, four advertisements per day and/or twenty advertisements per month. General advertisements might get priority claim on this time up to a set limit (say 75% of all advertisement time), with targeted advertisements next, and advisory messages last.

Another software enhancement that may be employed is software used for preference file management. Such "preference file management" software may, for example, include a default file which is periodically updated from the network server 114, and a Pocket Vault holder custom file. Using this software, the holder may, for example, be able to modify: (1)

the initial on-screen backdrop and message greeting; (2) the menu structure and media order within menu screens; (3) some (but not all) of the bio-metric input requirement parameters; (4) the amount of on-time after the bio-metric data is confirmed (within pre-set limits); (5) the ability to conceal all or part of the credit or debit account information on the Chameleon Card display area; (6) the normal restaurant tip percentage; (7) the links between certain media; and/or oversight preference restrictions.

For example, some of the menu tree structures for the Pocket Vault 102 may be set by the holder. This may include the sequence in which certain screens appear (e.g., debit screens before credit screens), among credit screens (e.g., Visa before MasterCard) and media order-of-appearance within a screen (e.g., FirstCard Visa before ChaseVisa).

Generally, a retailer does not need to see a credit or debit account number, while the approving entity contacted on the dialup modem does. Today, credit and debit cards have this information embossed on the card and recorded in the magnetic stripe on the back of the card. If the magnetically encoded information is unreadable due to mechanical wear of the magnetic stripe or for other reasons, the embossed image can always be read by the clerk and manually keyed in. There is no way for this embossing to disappear when it is not needed and appear at just the right time, either with a standard card or a Smartcard. As a result, such numbers are generally in view and this visibility may lead to fraud. In one embodiment, the Pocket Vault 102 may be programmed to conceal this number, unless prompted to the contrary by the holder. A retailer may confirm the kind of credit or debit being presented and the full name on the card, without having to see or be told the account number. On the rare occasion when the number itself is needed, the holder may, for example, repeat the bio-metric input to the Pocket Vault 102 to reveal the card account number. If placed in the personal interface station 104c, such account numbers may be automatically revealed (e.g., through detection of an encrypted cookie on the interface station computer 304 of the personal interface station 104c).

If the holder establishes a preferred tip percentage, this preferred tip amount may be automatically applied to restaurant checks. This may eliminate a step in restaurant check close-out and reduce the hassle of calculating an appropriate tip and eliminate the need for waitstaff to return to pick up the credit receipt with the tip.

The holder may also choose to link certain media on the Pocket Vault 102 to reduce selection tasks at the point-of-transaction. For example, the holder may link certain credit or

debit cards to certain frequent buyer ID cards, thereby enabling the holder to pick a grocery store frequent buyer card (which would be linked to a debit card and brought up automatically after the grocery store card).

At the point of registration or issuance, a Pocket Vault holder may be asked if there is to be any transaction oversight security. If the answer is yes, a second bio-metric input may be required from the individual endowed with that oversight role. For example, a parent may choose to get a Pocket Vault 102 for a child or other relative who may lack certain fiscal discipline. At issuance, and prior to any credit or debit media being added to the Pocket Vault 102, the oversight authority may need to be established. The person having such oversight authority may then have sole access to a profile of transaction preference data. The person having the oversight authority may therefore create and modify this profile any time after issuance. This data set may limit one or more of the following: (1) debit and credit transaction dollar volume per day, per week and/or per month; (2) certain purchase restrictions such as the types of retailers to whom payments are permitted, such as exclusion of gambling establishments or liquor stores; and (3) geographic restrictions such as payments within 10 miles of a son's or daughter's college campus, but not beyond).

Another software enhancement that may be employed is software for managing media image libraries. Every media image sent to the display 216 may actually be a composite of from two to five layers of graphics files. Layers one, two and four may, for example, be stored in media library files while layers three and five may include text and data files stored in memory on the Pocket Vault 102. For example, a credit card image may comprise separate layers for: (1) the standard credit card background and icon; (2) the issuing bank's overlay icons and text; (3) the individual's account number; and (4) customized advertising from the issuing bank and/or credit card company.

Layering the image in this fashion may minimize data transmission requirements, reduce memory storage requirements, and speed up screen display. For example, Pocket Vaults 102 may be preloaded at point of manufacture with background images of the top ten credit images, three passport images (e.g., EU, US, Japan), and a handful of other globally-relevant backgrounds. When, for example, a Pocket Vault holder living in Boston initially registers a device, it may trigger downloading of the top five additional background images prevalent in that area. When the individual applies for and is electronically issued a new credit card over the network system 100, the download from the network server 114 may

include a second layer credit card company overlay for the credit card, along with the third layer of account and name information, and the fourth layer of the most recent customized advertisement from the credit card company related to a seasonal promotion of card usage.

The advertisement layer may be temporary in nature. This layer may, for example, remain on-screen for a given number of seconds, predetermined by the time period of the advertisement paid for by the advertiser. Underneath such an advertisement, a fifth layer of Pocket Vault holder-determined data may appear, also for a temporary period, in this case for privacy reasons and for a period set by the holder. This positioning of the holder's data below the advertising data increase the value of the advertisement time, since holders will be likely to view the display 216 awaiting the appearance of their data, which may also remain on-screen for only a set number of second. For example, such holder-specific data may include the last date of the next billing period, or the total charges since the last billing period on this particular card or on all of the holder's credit cards. Such balance information may be generated, for example, by the financial management software. The initial on-screen image may also be layered, for example, with a market-tailored backdrop and a sign-on message, both of which possibly being modifiable could be modified by the appropriate setting of user preferences.

Another software enhancement that may be employed is software to manage memos. Certain screen choices may, for example, result in the viewing of memos created by and for the Pocket Vault holder. These memos may be written on a home PC and transferred to a Pocket Vault 102 when the Pocket Vault 102 is interfaced with the personal interface station 104c for an update/download session. Alternatively, such memos may be created on the Pocket Vault 102 using a screen-based keyboard function similar to that of a Palm Pilot. The memo template software may provide certain standard backgrounds and layouts to support this feature. This feature may help to eliminate the need for scraps of various notes now found in most wallets.

Yet another software enhancement that may be employed is software to manage advertising messages. Such advertising message management software may, for example, perform several noteworthy functions: (1) limiting the appearance of advertising in accordance with the advertising profile (e.g., stored in the network server 114) of the particular Pocket Vault holder; (2) limiting the appearance of advertising to a certain number of times per on-session, per hour, per day, per week and/or per month; (3) tracking the

number of times each advertisement appears since the last download/update session (since the number of on-sessions during any period will govern the number of opportunities certain advertisements have to run, this tracking may be necessary to enable billing of advertisers for actual advertisement exposure levels; (4) generating reminder advertisements for frequent buyer cards (e.g., a message such as "Ten weeks since your last car wash! One more and the next is free!"); and (5) tracking the effectiveness of advertising through linkage to the transaction files (e.g., the ability to build more accurate, comprehensive buying profiles since all of an individual's media are now "under one roof").

Another software enhancement that may be employed is software to process transaction data. Such transaction processing software may, for example, include the ability to track total outstanding transactions on particular media and compare those to media limits at the time of the next transaction, along with date validity of the media. If a particular piece of media is no longer valid, selection of this item from a menu may produce a message such as "expired," or "requires update to extend period of validity," or "payment of balance required before re-use."

Another software enhancement that may be employed is software to manage frequent buyer data. Such frequent buyer data management software may, for example, track purchases at stores with frequent buying programs that participate in the network system 100. This software may also indicate any frequent buyer credits that are about to expire or create advertisements that remind their Pocket Vault holders that they are about to qualify for a free item. For example, a tenth gasoline purchase at a service station/car wash may generate a message indicating that the holder is "now entitled to free car wash."

Yet another software enhancement that may be employed is software for managing financial information. This type of software may, for example, enable easy download advertisements into personal finance software used by some PC owners. It may also support certain on-board functionality in the Pocket Vault, such as charge card management, automatically shifting from the preferred credit card to another credit card, for example: (1) when a transaction would cause a credit limit to be exceeded, (2) when using a different card would lengthen the time after which actual payment would be due, (3) when using another card would garner desired contest eligibility, or maximize cash back points for a particular period, and/or (4) when use of another card would preclude having to pay annual dues.

Another software enhancement that may be employed is Global Positioning Software. Integration of this functionality with memo information and frequent buyer information may induce visits to nearby stores at convenient times to take advantage of sales, frequent buyer credits, etc.

Fig. 13 is a flow diagram illustrating an example implementation of a primary routine 1300 that may be executed by the controller 306 of the pocket vault interface unit 302 (Fig. 3).

As shown, the routine 1300 begins at a step 1346, wherein it is determined whether a card has been swiped through the stripe reader 315 of the interface unit 302.

When, at the step 1346, it is determined that a card has been swiped, the routine 1300 proceeds to a step 1348, wherein information from the swiped card read by the stripe reader 315 is transmitted to the interface station computer 304.

After the step 1348, the routine 1300 proceeds to a step 1302, wherein it is determined whether a first encrypted message has been received from the Pocket Vault 102 including an ID code that is released from the Pocket Vault 102 only upon proper user authentication (e.g., in response to a fingerprint match).

When, at the step 1346, it is determined that a card has not been swiped, the routine 1300 proceeds directly to the step 1302 (discussed above).

When, at the step 1302, it is determined that such a first encrypted message has not been received from the Pocket Vault 102, the routine 1300 proceeds to a step 1338, wherein it is determined whether any encrypted information and/or commands have been received from the interface station computer 304.

When, at the step 1338, it is determined that information and/or commands have been received from the interface station computer 304, the routine 1300 proceeds to a step 1340, wherein the received information and/or commands are forwarded to the Pocket Vault 102.

After the step 1340, the routine 1330 proceeds to a step 1342, wherein it is determined whether any information and/or commands have been received from the Pocket Vault 102.

When, at the step 1338, it is determined that no information or commands have been received from the interface station computer 304, the routine 1300 proceeds directly to the step 1342 (discussed above).

When, at the step 1342, it is determined that information and/or commands have been received from the Pocket Vault 102, the routine 1300 proceeds to a step 1344, wherein the received information and/or commands are forwarded to the interface station computer 304.

After the step 1344, the routine 1300 returns to the step 1346 (discussed above).

When, at the step 1342, it is determined that no information and/or commands have been received from the Pocket Vault 102, the routine 1300 proceeds directly to the step 1346.

When, at the step 1302, it is determined that a first encrypted message including a Pocket Vault ID has been received from the Pocket Vault 102, the routine 1300 proceeds to a step 1304, wherein the first encrypted message is forwarded to the interface station computer 304 (Fig. 3).

After the step 1304, the routine 1300 proceeds to steps 1306 and 1308, wherein it is determined whether a fingerprint has been scanned by the fingerprint scanner 316 of the pocket vault interface unit 302 before a timeout period measured by the step 1308 has elapsed.

When, at the steps 1306 and 1308, it is determined that a fingerprint has not been scanned within the timeout period of step 1308, the routine 1300 returns to the step 1346 (discussed above).

When, at the steps 1306 and 1308, it is determined that a fingerprint has been scanned by the fingerprint scanner 316 in a timely manner, the routine 1300 proceeds to a step 1310, wherein it is determined whether the scanned fingerprint matches a fingerprint stored in the memory 314 of the pocket vault interface unit 302.

When, at the step 1310, it is determined that the scanned fingerprint does match that of an authorized operator of the interface unit 302, the routine 1300 proceeds to a step 1312, wherein a second encrypted message, including an ID of the pocket vault interface unit 302 that is released only after a successful fingerprint match, is transmitted to the interface station computer 304.

After the step 1312, the routine 1300 returns to the step 1346 (discussed above).

When, at the step 1310, it is determined that the scanned fingerprint does not match any fingerprint stored in the memory 314 of the pocket vault interface unit 302, the routine 1300 proceeds to a step 1314, wherein a message is transmitted to the interface station computer 304 indicating there has been an unsuccessful attempt to authenticate an operator of the pocket vault interface unit 302.

After the step 1314, the routine 1300 proceeds to steps 1316 and 1318, wherein it is determined whether, before the expiration of a timeout period measured by the step 1318, a request has been received from the interface station computer 304 to add a new operator to the pocket vault interface unit 302.

When, at the steps 1316 and 1318, it is determined that such a request has not been received from the interface station computer 304 in a timely manner, the routine 1300 returns to the step 1302 (discussed above).

When, at the steps 1316 and 1318, it is determined that a request to add a new operator to the pocket vault interface unit 302 has been received from the interface station computer 304 in a timely manner, the routine 1300 proceeds to steps 1320 and 1322.

At the steps 1320 and 1322, it is determined whether three identical fingerprints have been stored in the interface unit 302 for each of the operator's two hands before the expiration of a timeout period measured by the step 1322. The operator may be prompted, e.g., on the display 324 of the interface station computer 304, to take appropriate steps to ensure his or her fingerprints are properly scanned. An example routine for obtaining the requisite fingerprint data from a user is discussed above in connection with steps 804a-810a and 804b-810b (for the Pocket Vault 102), and therefore will not be repeated here.

When, at the steps 1320 and 1322, it is determined that the requisite fingerprint information has not been stored in a timely manner, the routine 1300 proceeds to a step 1336, wherein an indication (e.g., a message or an audio tone) regarding the unsuccessful new operator validation attempt is generated.

After the step 1336, the routine 1300 returns to the step 1346 (discussed above).

When, at the steps 1320 and 1322, it is determined that the fingerprint information has been successfully stored in the interface unit 302 in a timely manner, the routine 1300 proceeds to a step 1324, wherein an encrypted message including an ID unique to the interface unit 302 is transmitted to the interface station computer 304 for ultimate registration with the network server 114.

After the step 1324, the routine 1300 proceeds to step 1326 and 1328, wherein is determined whether a message including validation information (e.g., a PKI certificate for the interface unit 302) has been received from the network server 114 (via the interface station computer 304) before the expiration of a timeout period.

When, at the steps 1326 and 1328, the validation information is not received by the interface unit 302 in a timely manner, the routine 1300 proceeds to the step 1336 (discussed above).

When, at the steps 1326 and 1328, it is determined that the validation information is received by the interface unit 302 in a timely manner, the routine 1300 proceeds to a step 1330, wherein the validation information is stored for the new operator.

After the step 1330, the routine 1300 proceeds to a step 1332, wherein an indication (e.g., a message or an audio tone) regarding the successful validation of the new operator is generated.

After the step 1332, the routine 1300 returns to the step 1346 (discussed above).

Fig. 14 is a flow diagram illustrating example implementation of a primary routine 1400 that may be executed by the controller 308 of the interface station computer 304 of Fig. 3.

As shown, the routine 1400 begins at a step 1402, wherein a menu is displayed on the display 324 of the interface station computer 304 that gives the operator of the interface station computer 304 several options to choose from. These options may, for example, include: (1) the option to request that a Pocket Vault 102 be validated (i.e., permitted to store a new finger print), (2) the option to request that the information currently stored on a Pocket Vault 102 be updated (e.g., information may be uploaded from the network server 114), (3) the option to request that a transaction involving a Pocket Vault 102 be authorized, and/or (4) the option to access a website on the network server 114 and take advantage of the functionality thereof.

It should be appreciated that the foregoing are only examples of menu options that may be provided to the operator of the interface station computer 304, and that the invention is not limited to the particular examples described. It should also be appreciated that fewer than all of the options shown may be provided in connection with different types of interface stations. For example, a validation interface station 104a may be provided only with option (1), a personal interface station may be provided only with option (2), and a commercial interface station may be provided only with option (3). In many instances, option (4) may be the only option required or desired to be employed by the user, as the website may itself provide all of the functionality of the other options (1)-(3). If fact, in such circumstances, the user need not be provided with a menu at all, as the user could simply log on the website

using a browser. An embodiment of a network system in which a website may be accessed by a server in this manner is discussed below in connection with Figs. 28-39.

After displaying the menu at the step 1402, the routine 1400 proceeds to a step 1404, wherein it is determined whether any requests to validate Pocket Vaults 102 have been received.

When, at the step 1404, it is determined that no request to validate a Pocket Vault 102 has been received, the routine 1400 proceeds to a step 1408, wherein it is determined whether any requests to update information on Pocket Vaults 102 have been received.

When, at the step 1408, it is determined that no request to update the information on a Pocket Vault 102 has been received, the routine 1400 proceeds to a step 1412, wherein it is determined whether any requests to authorize transactions involving Pocket Vaults 102 have been received.

When, at the step 1412, it is determined that no request to authorize a transaction involving a Pocket Vault 102 has been received, the routine 1400 proceeds to a step 1416, wherein it is determined whether the interface station computer has received any messages from Pocket Vault interface units 302 indicating that an unsuccessful operator authentication has occurred (i.e., the fingerprint of an operator scanned by the fingerprint scanner 316 has failed to match a fingerprint stored in the memory 314).

When, at the step 1416, it is determined that no such messages have been received, the routine 1400 proceeds to a step 1420, wherein it is determined whether a request to access a website on the network server 114 has been received.

When at the step 1420, it is determined that no request to access the website on the network server 114 has been received, the routine 1400 returns to the step 1402, wherein the menu of the various options for the operator is again displayed. Thus, the menu 1402 is displayed until one of the various options is selected in accordance with any of the steps 1404, 1408, 1412, 1416, or 1420.

When, at the step 1404, it is determined that a request to validate a Pocket Vault 102 has been received, the routine 1400 proceeds to a step 1406, wherein the PROCESS REQUEST TO VALIDATE POCKET VAULT routine (discussed below in connection with Fig. 15) is executed.

After the step 1406, the routine 1400 proceeds to the step 1408 (discussed above).

When, at the step 1408, it is determined that a request to update the information on a Pocket Vault 102 has been received, the routine 1410 proceeds to a step 1410, wherein the PROCESS REQUEST TO UPDATE INFO ON POCKET VAULT routine (discussed below in connection with Fig. 16) is executed.

After the step 1410, the routine 1400 proceeds to the step 1412 (discussed above).

When, at the step 1412, it is determined that a request to authorize a transaction involving a Pocket Vault 102 has been received, the routine 1400 proceeds to a step 1414, wherein the PROCESS REQUEST TO AUTHORIZE TRANSACTION routine (discussed below in connection with Fig. 17) is executed.

After the routine 1414, the routine 1400 proceeds to the step 1416 (discussed above).

When, at the step 1416, it is determined that a message has been received from an the interface station computer 304 indicating that an attempted fingerprint match of an operator has failed, the routine 1400 proceeds to a step 1418, wherein the PROCESS UNSUCCESSFUL OPERATOR AUTHENTICATION routine (discussed below in connection with Fig. 18) is executed.

After the routine 1418, the routine 1400 proceeds to the step 1420 (discussed above).

When, at the step 1420, it is determined that a request to access a website on the network server 114 has been received, the routine 1400 proceeds to a step 1422, wherein the PROCESS REQUEST TO ACCESS WEBSITE routine (discussed below in connection with Figs. 30-39) is executed.

After the step 1422, the routine 1400 returns to the step 1402 (discussed above).

Fig. 15 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO VALIDATE POCKET VAULT routine of Fig. 14 (step 1406).

As shown, the routine 1406 begins at a step 1502, wherein the potential new Pocket Vault holder is prompted to apply his or her fingerprint to the fingerprint scanner 220 of the Pocket Vault 102, and to interface the Pocket Vault 102 with the pocket vault interface unit 302. This may be accomplished, for example, by interfacing the docking interface 208 of the Pocket Vault 102 with the docking interface 312 of the pocket vault interface unit 302.

After the step 1502, the routine 1406 proceeds to steps 1504 and 1506, wherein it is determined whether an encrypted message including the ID of the Pocket Vault 102 has been received from the pocket vault interface unit 302 prior to the expiration of a timeout period measured by the step 1506.

When, at the steps 1504 and 1506, it is determined that an encrypted message including the ID of the Pocket Vault 102 has not been received from the pocket vault interface unit 302 in a timely manner, the routine 1406 proceeds to a step 1526, wherein a message is displayed on the display 324 of the interface station computer 304 indicating that an error has occurred in the Pocket Vault validation process.

When, at the steps 1504 and 1506, it is determined that an encrypted message including the ID of the Pocket Vault 102 has been received from the pocket vault interface unit 302 in a timely manner, the routine 1406 proceeds to a step 1506, wherein the interface station operator is prompted to apply his or her fingerprint to the fingerprint scanner 316 of the pocket vault interface unit 302.

After the step 1506, the routine 1406 proceeds to steps 1508 and 1510, wherein it is determined whether an encrypted message including the ID of the pocket vault interface unit 302 has been received from the pocket vault interface unit 302 prior to the expiration of a timeout period measured by the step 1510.

When, at the steps 1508 and 1510, it is determined that an encrypted message including the ID of the pocket vault interface unit 302 has not been received from the pocket vault interface unit 302 in a timely manner, the routine 1406 proceeds to the step 1526, wherein a message is displayed on the display 324 of the interface station computer 304 indicating that the attempt to authorize the interface station operator was unsuccessful.

After the step 1526, the routine 1406 terminates.

When, at the steps 1508 and 1510, it is determined that an encrypted message including the ID of the pocket vault interface unit 302 has been received from the pocket vault interface unit 302 in a timely manner, the routine 1406 proceeds to a step 1512, wherein the interface station operator is prompted to input information regarding the new Pocket Vault holder into the interface station computer 304.

After the step 1512, the routine 1406 proceeds to a step 1514, whereat the routine 1406 waits until all of the requisite information regarding the new Pocket Vault holder has been entered properly (e.g., via the user input device 318 of the interface station computer 304).

After the step 1514, the routine 1406 proceeds to a step 1516, wherein the network server 114 (Fig. 1) is contacted.

After the step 1516, the routine 1406 proceeds to a step 1518, wherein the information regarding the new Pocket Vault holder is transmitted to the network server 114, along with a request that the new Pocket Vault holder be validated.

After the step 1518, the routine 1406 proceeds to steps 1520 and 1522, wherein it is determined whether the network server 114 has acknowledged the request by the interface station computer 304 prior to the expiration of a timeout period measured by the step 1522.

When, at the steps 1520 and 1522, it is determined that the network server 114 has not acknowledged the request by the interface station computer 304 in a timely manner, the routine 1406 proceeds to a step 1524, wherein a message is displayed on the display 324 indicating that a transmission failure has occurred.

When, at the steps 1520 and 1522, it is determined that the network server 114 has acknowledged the request by the interface station computer 304 in a timely manner, the routine 1406 proceeds to a step 1528, wherein, in an encrypted format, the information regarding the new Pocket Vault holder is transmitted to the network server 114, along with the interface station operator ID, the interface unit ID, and the Pocket Vault ID.

After the step 1528, the routine 1406 proceeds to steps 1530 and 1532, wherein it is determined whether encrypted validation information (e.g., a PKI certificate) has been received from the network server 114 prior to the expiration of a timeout period measured by the step 1532, and prior to receiving a message from the network server 114 indicating that the request to validate the new Pocket Vault holder has been denied.

When, at the steps 1530 and 1532, it is determined that encrypted validation information has not been received from the network server 114 in a timely manner, or it is determined that a message has been received indicating that the request to validate the new Pocket Vault holder has been denied, the routine 1406 proceeds to a step 1538, wherein a message is displayed on the display 324 indicating that the attempt to validate the Pocket Vault 102 was unsuccessful.

When, at the steps 1530 and 1532, it is determined that encrypted validation information has been received from the network server 114 in a timely manner, the routine 1406 proceeds to a step 1534, wherein the encrypted validation information (e.g., a PKI certificate) from the network server 114 is forwarded to the pocket vault interface unit 302 for forwarding on to the Pocket Vault 102.

After the step 1534, the routine 1406 proceeds to a step 1536, wherein a message is displayed on the display 324 indicating that the attempt to validate the Pocket Vault 102 was successful. In addition to this message, when the pocket vault interface unit 302 forwards this message on to the Pocket Vault 102, the Pocket Vault 102 itself may provide, for example, an audio indication such as a chime, indicating that the Pocket Vault 102 has been successfully validated.

Fig. 16 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO UPDATE INFO ON POCKET VAULT routine of Fig. 14 (step 1410).

As shown, the routine 1410 begins at a step 1602, wherein the Pocket Vault holder is prompted to apply his or her fingerprint to the fingerprint scanner 220 of the Pocket Vault 102, and to interface the Pocket Vault 102 with the pocket vault interface unit 302.

After the step 1602, the routine 1410 proceeds to steps 1604 and 1606, wherein it is determined whether an encrypted message including the ID of the Pocket Vault 102 has been received from the pocket vault interface unit 302 prior to the expiration of a timeout period measured by the step 1606.

When, at the steps 1604 and 1606, it is determined that an encrypted message including the ID of the Pocket Vault 102 has not been received from the pocket vault interface unit 302 in a timely manner, the routine 1410 proceeds to a step 1634, wherein a message is displayed on the display 324 of the interface station computer 304 indicating that the attempt to authorize the Pocket Vault holder was unsuccessful.

When, at the steps 1604 and 1606, it is determined that an encrypted message including the ID of the Pocket Vault 102 has been received from the pocket vault interface unit 302 in a timely manner, the routine 1410 proceeds to a step 1606, wherein the interface station operator is prompted to apply his or her fingerprint to the fingerprint scanner 316 of the pocket vault interface unit 302.

After the step 1606, the routine 1410 proceeds to steps 1608 and 1610, wherein it is determined whether an encrypted message including the ID of the pocket vault interface unit 302 has been received from the pocket vault interface unit 302 prior to the expiration of a timeout period measured by the step 1610.

When, at the steps 1608 and 1610, it is determined that an encrypted message including the ID of the pocket vault interface unit 302 has not been received from the pocket vault interface unit 302 in a timely manner, the routine 1410 proceeds to the step 1634,

wherein a message is displayed on the display 324 of the interface station computer 304 indicating that the attempt to authorize the interface station operator was unsuccessful.

After the step 1634, the routine 1410 terminates.

When, at the steps 1608 and 1610, it is determined that an encrypted message including the ID of the pocket vault interface unit 302 has been received from the pocket vault interface unit 302 in a timely manner, the routine 1410 proceeds to a step 1612, wherein the network server 114 is contacted.

After the step 1612, the routine 1410 proceeds to a step 1614, wherein a request to update the information on the Pocket Vault 102 is transmitted to the network server 114.

After the step 1614, the routine 1410 proceeds to steps 1616 and 1618, wherein it is determined whether the network server 114 has acknowledged the request by the interface station computer 304 prior to the expiration of a timeout period measured by the step 1618.

When, at the steps 1616 and 1618, it is determined that the network server 114 has not acknowledged the request by the interface station computer 304 in a timely manner, the routine 1410 proceeds to a step 1620, wherein a message is displayed on the display 324 indicating that a transmission failure has occurred.

When, at the steps 1616 and 1618, it is determined that the network server 114 has acknowledged the request by the interface station computer 304 in a timely manner, the routine 1410 proceeds to a step 1622, wherein, in an encrypted manner, the interface station operator ID, the interface unit ID, and the Pocket Vault ID are transmitted to the network server 114.

After the step 1622, the routine 1410 proceeds to steps 1624 and 1626, wherein it is determined whether encrypted updates have been received from the network server 114 for loading onto the Pocket Vault 102 prior to the expiration of a timeout period measured by the step 1620, and prior to the network server 114 denying the requested attempt to upload information.

When, at the steps 1624 and 1626, it is determined that the encrypted updates have been received in a timely manner, the routine 1410 proceed to a step 1630, wherein the received updates are transmitted to the pocket vault interface unit 302 so that they may be subsequently forwarded to the Pocket Vault 102 for uploading thereto.

After the step 1630, the routine 1410 proceeds to a step 1632, wherein a message is displayed to the holder indicating that the requested updates have been successfully uploaded to the Pocket Vault 102.

After the step 1632, the routine 1410 terminates.

When, at the steps 1624 and 1626, it is determined that the encrypted updates have not been received from the network server 114 in a timely manner, or that the network server 114 has denied the request to upload information onto the Pocket Vault 102, the routine 1410 proceeds to a step 1628, wherein a message is displayed on the display 324 indicating that the attempt to update the information on the Pocket Vault 102 was unsuccessful.

After the step 1628, the routine 1410 terminates.

Fig. 17 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO AUTHORIZE TRANSACTION routine of Fig. 14 (step 1414).

As shown, the routine 1414 begins at a step 1702, wherein the operator of the interface station computer 304 is prompted to input information regarding the proposed transaction involving the Pocket Vault 102.

After the step 1702, the routine 1414 waits at a step 1704 until all of the information regarding the requested transaction has been entered.

After, at the step 1704, it is determined that all of information regarding the requested transaction has been entered, the routine 1414 proceeds to a step 1706, wherein the Pocket Vault holder is prompted to apply his or her fingerprint to the fingerprint scanner 220 of the Pocket Vault 102, and to interface the Pocket Vault with the pocket vault interface unit 302.

After the step 1706, the routine 1414 proceeds to steps 1708 and 1710, wherein it is determined whether an encrypted message including the ID of the Pocket Vault 102 has been received from the pocket vault interface unit 302 prior to the expiration of a timeout period measured by the step 1710.

When, at the steps 1708 and 1710, it is determined that an encrypted message including the ID of the Pocket Vault 102 has not been received from the pocket vault interface unit 302 in a timely manner, the routine 1414 proceeds to a step 1726, wherein a message is displayed on the display 324 of the interface station computer 304 indicating that the attempt to authorize the Pocket Vault holder was unsuccessful.

When, at the steps 1708 and 1710, it is determined that an encrypted message including the ID of the Pocket Vault 102 has been received from the pocket vault interface

unit 302 in a timely manner, the routine 1414 proceeds to a step 1712, wherein the interface station operator is prompted to apply his or her fingerprint to the fingerprint scanner 316 of the pocket vault interface unit 302.

After the step 1712, the routine 1414 proceeds to steps 1714 and 1715, wherein it is determined whether an encrypted message including the ID of the pocket vault interface unit 302 has been received from the pocket vault interface unit 302 prior to the expiration of a timeout period measured by the step 1715.

When, at the steps 1714 and 1715, it is determined that an encrypted message including the ID of the pocket vault interface unit 302 has not been received from the pocket vault interface unit 302 in a timely manner, the routine 1414 proceeds to the step 1726, wherein a message is displayed on the display 324 of the interface station computer 304 indicating that the attempt to authorize the interface station operator was unsuccessful.

After the step 1726, the routine 1414 terminates.

When, at the steps 1714 and 1715, it is determined that an encrypted message including the ID of the pocket vault interface unit 302 has been received from the pocket vault interface unit 302 in a timely manner, the routine 1414 proceeds to a step 1716, wherein the network server 114 is contacted.

After the step 1716, the routine 1414 proceeds to a step 1718, wherein the request regarding the proposed transaction involving the Pocket Vault 102 is transmitted to the network server 114.

After the step 1718, the routine 1414 proceeds to step 1720 and 1722, wherein it is determined whether the transaction request has been acknowledged by the network server 114 before the expiration of a timeout period measured by the step 1722.

When, at the steps 1720 and 1722, it is determined that the request has not been acknowledged in a timely manner, the routine 1414 proceeds to a step 1724, wherein a message is displayed on the display 324 indicating that a transmission failure has occurred.

After the steps 1724, the routine 1414 terminates.

When, at the steps 1722 and 1724, it is determined that the request has been acknowledged in a timely manner, the routine 1414 proceeds to a step 1728, wherein encrypted information about the requested transaction is transmitted to the network server 114, along with the interface station operator ID, the interface unit ID, and the Pocket Vault ID.

After the step 1728, the routine 1414 proceeds to steps 1730 and 1732, wherein it is determined whether an encrypted transaction approval message has been received from the network server 114 prior to the expiration of a timeout period measured by the step 1732.

When, at the steps 1730 and 1732, it is determined that an encrypted transaction approval message has not been received in a timely manner, or that approval for the requested transaction has been denied by the network server 114, the routine 1414 proceeds to a step 1736, wherein a message is displayed on the display 324 indicating that the attempt to authorize the requested transaction has failed.

When , at the steps 1730 and 1732, it is determined that an encrypted transaction approval message has been received in a timely manner, the routine 1414 proceeds to a step 1734, wherein a message is forwarded to the pocket vault interface unit 302 indicating that the requested transaction has been approved. This message may also be used to update information on the Pocket Vault 102, and/or to cause the Pocket Vault 102 to generate an indication (e.g., an audio tone) that the transaction has been approved.

After the step 1734, the routine proceeds to a step 1738, wherein a message is displayed on the display 324 indicating that the requested transaction has been approved.

After the step 1738, the routine 1414 terminates.

Fig. 18 is a flow diagram illustrating an example implementation of the PROCESS UNSUCCESSFUL OPERATOR AUTHENTICATION routine of Fig. 14 (step 1418).

As shown, the routine 1418 begins at a step 1802, wherein the operator of the interface station computer 304 is informed that the attempted use the pocket vault interface unit 302 (when the operator applied his or her finger print to the fingerprint scanner 316) was not authorized.

After the step 1802, the routine 1418 proceeds to a step 1804, wherein the operator is prompted to either: (1) add a NEW OPERATOR to the interface unit 302, or (2) ABORT the attempt to use the interface unit 302.

When, at the step 1806, it is determined that the operator has chosen to ABORT the attempt to use the interface unit 302, the routine 1418 terminates.

When, at the step 1806, it is determined that the operator has chosen to add a NEW OPERATOR, the routine 1418 proceeds to a step 1808, wherein a message is transmitted to the pocket vault interface unit 302 indicating the operator's desire to add a new operator to the pocket vault interface unit 302.

After the step 1808, the routine 1418 proceeds to a step 1810, wherein the operator is prompted to input information regarding the proposed new operator into the interface station computer 304 (e.g., using the user input device 318), and is provided with instructions as to the application of three identical fingerprints from each of his or her two hands to the fingerprint scanner 316 of the interface unit 302.

After the step 1810, the routine 1418 proceeds to a step 1812 wherein the routine 1418 waits until all of the requisite information regarding the proposed new interface station operator has been entered properly.

When, at the step 1812, it is determined that all of the requisite information regarding the proposed new operator has been entered properly, the routine 1418 proceeds to a step 1814, wherein the network server 114 is contacted.

After the step 1814, the routine 1418 proceeds to a step 1816, wherein the request to add the new operator to the pocket vault interface unit 302 is transmitted to the network server 114.

After the step 1816, the routine 1418 proceeds to steps 1818 and 1820, wherein it is determined whether the request by the interface station computer has been acknowledged by the network server 114 prior to the expiration of a timeout period measured by the step 1820.

When, at the steps 1818 and 1820, it is determined that the request has not been acknowledged in a timely manner, the routine 1418 proceeds to the step 1822, wherein a transmission failure message is displayed.

After the step 1822, routine 1418 terminates.

When, at the steps 1818 and 1820, it is determined that the request has been acknowledged in a timely manner, the routine 1418 proceeds to the step 1824, wherein a message, including the information regarding the proposed new operator and the interface unit ID, is transmitted to the network server 114 in an encrypted manner.

After the step 1824, the routine 1418 proceeds to steps 1826 and 1828, wherein it is determined whether encrypted validation information (e.g., a PKI certificate) has been received from the network server 114 prior to the expiration of a timeout period measured by the step 1828, and prior to the network server 114 denying the addition of the new interface station operator.

When, at the steps 1826 and 1828, it is determined that encrypted validation information has been received from the network server 114 in a timely manner, the routine

1418 proceeds to a step 1830, wherein the encrypted validation information (e.g., a PKI certificate) is forwarded from the interface station computer 304 to the pocket vault interface unit 302.

After the step 1830, the routine 1418 proceeds to a step 1834, wherein a message is generated indicating that the attempt to add the new operator to the pocket vault interface unit 302 was successful.

After the step 1834, the routine 1418 terminates.

When, at the steps 1826 and 1828, it is determined that encrypted validation information has not been received from the network server 114 in a timely manner, the routine 1418 proceeds to a step 1832, wherein a message is generated indicating that the attempt to add the new operator to the pocket vault interface unit 302 was unsuccessful.

After the step 1832, routine 1418 terminates.

Fig. 19 is a flow diagram illustrating an example implementation of a primary routine 1900 that may be executed by the network server 114 of Fig. 1.

As shown, the routine 1900 may begin at a step 1902, wherein it is determined whether any requests have been received to register new Pocket Vault holders.

When, at the step 1902, it is determined that a request has been received to register a new Pocket Vault holder, the routine 1900 proceeds to a step 1904, wherein the request to register the new Pocket Vault holder is processed. An example of a routine that may be employed to implement the step 1904 is discussed in more detail below in connection with Fig. 20.

When, at the step 1902, it is determined that no request to register a new Pocket Vault holder has been received, the routine 1900 proceeds to a step 1906, wherein consumer marketing information is compiled and transmitted to subscribing media issuers and advertisers.

After the step 1906, the routine 1900 proceeds to a step 1908, wherein it is determined whether any requests from media issuers or advertisers have been received to update the network server 114.

According to one aspect of the invention, media issuers and advertisers may have the option to utilize the functionality of the network server 114 to update the account characteristics of authenticated Pocket Vault holders. These updates may, for example, be delivered from the computers 108, 110, and 112 to a secure location within the database 406.

When each selected holder next synchronizes with network server 114 (e.g., as described below in connection with routine 1914 of Fig. 22), any media characteristics updated by the media issuers or advertisers may be uploaded to that holder's the Pocket Vault 102. The database of account updates may be revised periodically based on the media issuer's systems (e.g., pursuant to the routine 1910 of Fig. 21 - described below). Confirmation of the update process may be provided to the issuer after a synchronization session is complete for a particular Pocket Vault holder (see step 2206 of routine 1914 (Fig. 22) below).

When, at the step 1908, it is determined that a request to update the network server 114 has been received from a media issuer or advertiser, the routine 1900 proceeds to a step 1910, wherein the request from the media issuer or advertiser is processed. An example of a routine that may be employed to implement the step 1910 is discussed in more detail below in connection with Fig. 21.

When, at the step 1908, it is determined that no request from a media issuer or advertiser to update the network server 114 has been received, the routine 1900 proceeds to a step 1912, wherein it is determined whether any requests have been received from holders to update information on their Pocket Vaults.

When, at the step 1912, it is determined that such a request has been received, the routine 1900 proceeds to a step 1914, wherein the request to update the Pocket Vault information is processed. An example of a routine that may be employed to implement the step 1914 is described in more detail below in connection with Fig. 22.

When, at the step 1912, it is determined that no request from a holder to update information on a Pocket Vault 102 has been received, the routine 1900 proceeds to a step 1916, wherein it is determined whether any holders have requested that new files be loaded onto the network server 114.

When, at the step 1916, it is determined that a holder has requested that a new file be loaded onto the network server 114, the routine 1900 proceeds to a step 1918, wherein the holder's request to load the new file onto the network server 114 is processed. An example of a routine that may be employed to implement the step 1918 is described in more detail below in connection with Fig. 23.

When, at the step 1916, it is determined that no request by a holder to load a file onto the network server 114 has been received, the routine 1900 proceeds to a step 1920, wherein it is determined whether any requests have been made to authorize transactions. Such a

request may be made, for example, by a merchant operating a commercial interface station 104c. In this regard, it should be appreciated that, when a token 102a is employed to engage in a transaction with a commercial card reader 106 or a commercial bar code reader 107, a request for transaction approval may not be made to the network server 114. Instead such a transaction approval request may be made through conventional, existing communication and approval channels for such devices. Therefore, it should be understood that the step 1922 is generally reached only when it is possible for the network server 114 to check the identity of the Pocket Vault holder, the identity of the Pocket Vault 102, and possibly identity of the operator of a commercial interface station, based on communications with the Pocket Vault 102 (e.g., via a commercial interface station 104c or via a wireless network such as Bluetooth).

When, at the step 1920, it is determined that a request to authorize a transaction has been made, routine 1900 proceeds to a step 1922, wherein the request to authorize the transaction is processed. An example of a routine that may be employed to implement the step 1922 is discussed in more detail below in connection with Fig. 24.

When, at the step 1920, it is determined no request to authorize a transaction has been made, the routine 1900 returns to the step 1902 (discussed above). With regard to the routine 1900 of Fig. 19, it should be appreciated that all of the requests to accomplish the various tasks may be placed in a queue so that they are serviced on a first-come, first-served or any other basis, rather than servicing them in the particular order shown in Fig. 19.

Fig. 20 is a flow-diagram illustrating an example of a routine that may be employed to implement the step 1904 of the routine 1900 (Fig. 1).

As shown, the routine 1904 begins at a step 2002, wherein a request received from the interface station computer 304 to register a new Pocket Vault holder is acknowledged, and the network server 114 requests the interface station computer 304 to transfer the relevant information regarding the proposed new holder to the network server 114.

After the step 2002, the routine 1904 proceeds to a step 2004, wherein the routine 1904 waits for all of the requisite holder registration information to be received from the interface station computer 304.

When, at the step 2004, it is determined that all of the requisite holder registration information has been received from the interface station computer 304, the routine 1904 proceeds to a step 2006, wherein it is determined whether the proposed Pocket Vault use is

authorized. An example of a routine that may be employed to implement the step 2006 is discussed below in connection with Fig. 25. In determining whether a particular Pocket Vault use is authorized, there are numerous parameters which may be checked. For example, the port to which the interface station computer is connected (e.g., the telephone number or IP address of the computer) may be checked to ensure that it is authorized. Additionally, information from the interface station computer 304 (e.g., a "cookie") may be checked to ensure that the computer itself has been registered with the system. Further, it can be checked whether the current operator of the interface station computer 304 is registered as being associated with the interface station computer 304 being used, and that the proposed new Pocket Vault holder is authorized to use that particular the Pocket Vault 102. In sum, the identity of (1) each piece of equipment, (2) each operator of each piece of equipment, and (3) each location of each piece of equipment may be checked to ensure that the particular use of the Pocket Vault is authorized. It should be appreciated fewer than all of these parameters, different parameters, and/or additional parameters can be checked in alternative embodiments of the invention, and that the invention is not limited to embodiments wherein all of the aforementioned parameters are checked to verify that a particular Pocket Vault use is authorized.

When, at the step 2006, it is determined that the Pocket Vault use is not authorized, the routine 1904 terminates. In such a situation, it is also possible to generate some sort of security alert message to put someone or some entity on notice that an unauthorized use of a Pocket Vault has occurred.

When, the routine 2006 has determined that the proposed Pocket Vault use is authorized, the routine 1904 proceeds to a step 2008, wherein all of the relevant information regarding the new Pocket Vault registration is logged into the database 406 of the network server 114 (Fig. 4). As shown in Fig. 20, this information may include, for example, the interface station operator ID, the interface unit ID, the Pocket Vault ID, and all of the relevant information relating to the new Pocket Vault holder.

After the step 2008, the routine 1904 proceeds to a step 2010, wherein the network server 114 transmits encrypted validation information to the interface station computer 304, which then may be passed on to the pocket vault interface unit 302, and then to the Pocket Vault 102, so as to enable the new holder's fingerprint to be stored in the memory of the Pocket Vault 102.

After the step 2010, the routine 1904 terminates.

Fig. 21 is a flow diagram illustrating example of a routine that may be employed to implement the step 1910 of the primary routine 1900 (Fig. 19).

As shown, the routine 1910 begins at a step 2102, wherein it is determined whether all of the requested updates have been received from the media issuer or advertiser.

When, at the step 2102, it has been determined that all of the requested updates have been received, the routine 1910 proceeds to a step 2104, wherein it is determined whether the media issuer or advertiser is authorized access to the network server 114. This authorization process may require some sort of authentication of the identity of the computer used by the media issuer or advertiser requesting the update, the operator of the computer, and/or the location of the computer, in a manner similar to that in which the interface stations 104 and their operators are authorized.

When, at the step 2104, it is determined that the media issuer or advertiser is not authorized access to the network server 114, the routine 1900 proceeds to a step 2106, wherein a message is transmitted to the media issuer or advertiser informing the media issuer or advertiser that access to the network server 114 has been denied.

After the step 2106, the routine 1910 terminates.

When, at the step 2104, it is determined that the media issuer or advertiser is authorized access to the network server 114, the routine 1910 proceeds to a step 2108, wherein the updates received from the media issuer or advertiser are logged onto the network server 114.

After the step 2108, the routine 1910 terminates.

Fig. 22 is a flow diagram illustrating an example a routine that may be employed to implement the step 1914 of the primary routine 1900 (Fig. 19).

As shown, the routine 1914 begins at the step 2006 (discussed below in connection with Fig. 25), wherein it is determined whether the attempted Pocket Vault use is authorized.

When, at the step 2006, it is determined that the Pocket Vault use is not authorized, the routine 1914 terminates.

When, at the step 2006, it is determined that the Pocket Vault use is authorized, the routine 1914 proceeds to a step 2202, wherein encrypted updates are transmitted to the interface station computer 304 for loading onto the Pocket Vault 102.

After the step 2202, the routine 1914 proceeds to steps 2204 and 2206, wherein the time and date of the updates are logged (step 2204), and the media issuers or advertisers are informed that the updates have been made (step 2206).

Fig. 23 is a flow diagram illustrating an example of a routine that may be employed to implement the step 1918 of the primary routine 1900 (Fig. 9).

As shown, the routine 1918 begins at a step 2302, wherein it is determined whether the file to be loaded onto the network server 114 relates to a secure media issuer.

When, at the step 2302, it is determined that the file does not relate to a secure media issuer, the routine 1918 proceeds to a step 2304, wherein the network server 114 is updated with the non-secure file.

After the step 2304, the routine 1918 terminates.

When, at the step 2302, it is determined that the to-be-loaded file does relate to a secure media issuer, the routine 1918 proceeds to a step 2306, wherein it is determined whether the secure media issuer is a Pocket Vault participant (i.e., a media issuer having access to the network server 114).

When, at the step 2306, it is determined that the secure media issuer is not a Pocket Vault participant, the routine 1918 proceeds to a step 2308, wherein an advisory is sent to the holder indicating an inability to load the file, and inquiring as to whether the holder desires to load the file in a non-secure format. The holder may, for example, opt to load the file to the network server 114 in such a way that the content of the file is not encodable to the Chameleon Card, but can be displayed and shown to a POS operator and manually keyed in at POS by the POS operator.

After the step 2308, the routine 1918 proceeds to a step 2316, wherein it is determine whether the holder has elected to load the file in a non-secure format.

When, at the step 2316, it is determined that the holder has elected not to load the file in a non-secure format, the routine 1918 terminates.

When, at the step 2316, it is determined that the holder has elected to load the file in a non-secure format, the routine 1918 proceeds to a step 2318, wherein the file is loaded onto the network server 114 in a non-secure format.

After the step 2318, the routine 1918 terminates.

When, at the step 2306, it is determined that the secure media issuer is a Pocket Vault participant, the routine 1918 proceeds to a step 2310, wherein the media issuer is queried as to the account status of the holder.

After the step 2310, the routine 1918 proceeds to a step 2312, wherein it is determined whether authorization has been received from the media issuer to load the file.

When, at the step 2312, it is determined that authorization has not been received from the media issuer, the routine 1918 proceeds to the step 2308 (discussed above).

When, at the step 2312, it is determined that authorization has been received from the media issuer, the routine 1918 proceeds to a step 2314, wherein the network server 114 is updated with the secure file.

After the step 2314, the routine 1918 terminates.

Fig. 24 is a flow diagram illustrating an example of a routine that may be employed to implement the step 1922 of the primary routine 1900 (Fig. 19).

As shown, the routine 1922 begins at the step 2006 (discussed below in connection with Fig. 25), wherein it is determined whether the attempted use of the Pocket Vault 102 is authorized.

When, at the step 2006, it is determined that the attempted Pocket Vault use is not authorized, the routine 1922 terminates.

When, at the step 2006, it is determined that the attempted Pocket Vault used is authorized, the routine 1922 proceeds to a step 2402, wherein it is determined whether the requested transaction is within acceptable account parameters (e.g., as set by the media issuer).

When, at the step 2402, it is determined that the requested transaction is not within acceptable account parameters, the routine 1922 proceeds to a step 2404, wherein a message is transmitted to the entity that requested the transaction (e.g., a commercial interface station 104C, a card reader 106, or a barcode reader 107) indicating that the transaction is outside of acceptable account parameters.

After the step 2404, the routine 1922 terminates.

When, at the step 2402, it is determined that the requested transaction is within acceptable account parameters, information regarding the transaction is logged into the database 406 of the network server 114 (Fig. 4). As shown, the logged information may

include the identification of the entity with which the transaction took place, the Pocket Vault ID (if available), and the time and date of the transaction.

After the step 2406, the routine 1922 proceeds to a step 2408, wherein an encrypted approval message is transmitted to the entity with which the transaction is being attempted (e.g., a commercial interface station 104C, a card reader 106, or a barcode reader 107).

After the step 2408, the routine 1922 terminates.

Fig. 25 is a flow diagram illustrating an example of a routine that may employed to implement the step 2006 of the routines 1904 (Fig. 20), 1914 (Fig. 22), and 1922 (Fig. 24).

As shown, the routine 2006 begins at a step 2502, wherein it is determined whether the point of sale terminal or other entity with which a transaction is being attempted is connected to a valid source (e.g., an authorized telephone line or an authorized internet protocol (IP) address).

When, at the step 2502, it is determined that the entity proposing the transaction is not connected to a valid source, the routine 2006 proceeds to a step 2510, wherein the transaction is refused, and a security alert is generated so that appropriate action(s) may be taken.

When, at the step 2502, it is determined that the entity proposing the transaction is connected to a valid source, the routine 2006 proceeds to a step 2504, wherein it is determined whether the ID of the interface station, card reader or barcode reader is valid, and is properly linked to the source to which is connected.

When, at the step 2504, it is determined that the ID of the entity proposing the transaction is not valid, the routine proceeds to the step 2510 (discussed above).

When, at the step 2504, it is determined that the ID of the entity proposing the transaction is valid, the routine 2006 proceeds to a step 2506, wherein it is determined whether the Pocket Vault ID (if available) is valid. It should be appreciated that, when a card reader 106, a barcode reader 107 or an RF signal receiver is employed, it is possible that the ID from the Pocket Vault will not be transmitted to the network server 114. Therefore, the step 2506 may be skipped in such a situation.

When, at the step 2506, it is determined that the Pocket Vault ID (when available and required) is not valid, the routine 2006 proceeds to the step 2510 (discussed above).

When, at the step 2506, it is determined that the Pocket Vault ID (when) is valid or is not required, the routine 2006 proceeds to a step 2508, wherein it is determined whether the

Pocket Vault ID (if available) is linked to the ID of the entity proposing the transaction, e.g., a commercial interface station 104c, a card reader 106, or a barcode reader 107.

When, at the step 2508, it is determined that the ID of the Pocket Vault 102 (when available) is not linked to the ID of the entity proposing the transaction, the routine 2006 proceeds to the step 2510 (discussed above).

When, at the step 2508, it is determined that the Pocket Vault ID is linked to the ID of the entity proposing the transaction, or that the ID of the Pocket Vault is not required, the routine 2006 proceeds to a step 2512, wherein the Pocket Vault use is authorized.

With regard to the information checked in connection with the routine 2006 to determine whether a particular Pocket Vault use is authorized, it should be appreciated that, in some embodiments, fewer than all of the verification steps discussed above may be performed when lesser degrees of security are desired or required. For example, in some embodiments, there may be no restrictions as to who can operate an interface station, the source to which the station is connected, and/or the ID of the station.

Figure 27 illustrates a network system similar to that described hereinabove. The system of Fig. 27, however, includes several additional components which serve to increase the network's functionality and utility. Accordingly, it should be appreciated that, in addition to the components illustrated in Fig. 27, the system may also include all or some of the components and features of the system described above in connection with Figs. 1-26, and may also incorporate all or some of that system's functionality.

As shown in Fig. 27, the Pocket Vault 102 may be coupled to an interface station 104 (including an interface unit 302 coupled to an the interface station computer 304). The interface unit 302 may include a communication port 2706, which is adapted to perform basic communications functions for interaction between the interface unit 302 and each of the Pocket Vault 102 and the interface station computer 304. This communication can take place over physical wires using a USB protocol or HotWire, or any other suitable protocol. Alternatively, the communication can be wireless, using a standard wireless protocol, such as Bluetooth, or any other suitable protocol. The communication port 2706 may, of course, be adapted to perform communications functions depending on the requirements on the particular protocol used. In an example embodiment, a USB protocol is used, and the interface unit 302 is connected to the interface station computer 304 through a USB port.

Several suitable methods/techniques for interfacing the Pocket Vault 102 with the interface unit 302 are described above.

In addition to the communication port 2706, as in the embodiment described above, the interface unit 302 contains a stripe reader 315. The purpose and operation of the stripe reader 315 is described below in connection with Figure 34.

The interface station computer 304 may be any suitable computer that employs one or more processors to execute instructions stored in memory. The interface station computer 304 may even comprise several inter-networked computers.

In the illustrative embodiment shown, the interface station computer 304 may use the communication software 2710 to communicate with the network server 114 via the network 2724. The communication software 2710 may be any of a number of communication programs known in the art, and the invention is not limited to any particular type of software. The software 2710 may, for example, comprise a web browser, a terminal emulation program, a proprietary program, or any other software module capable of communicating with other computers using the network 2724. The network 2724 may be any communication network known in the art. For example, the network 2724 may comprise the World Wide Web, a Local Area Network, or any other networking arrangement adapted for communication between digital computers.

In the embodiment shown, the communication software 2710 uses internet settings 2722 when accessing the network 2724. The internet settings 2710 may include any user preferences or software settings relevant to communication functions and usability of the communication software 2710. The internet settings 2722 may comprise, for example, the network name and the identification of the interface station computer 304, an identification of communications protocols used to connect to the network 2724, network preferences, such as whether any proxy servers may or should be used, a list of frequently-used servers, cookies previously obtained from various websites, digital certificates, personal bookmarks, user identity data, user password data for various servers, etc.

The communication software 2710 may access the network 2724 through communication protocol layer 2714. Depending on how the interface station computer 304 is physically connected to the network 2724. The communication protocol layer 2714 may be dial-up software, a TCP/IP layer, or any other suitable networking layer. The communication protocol layer 2714 may, for example, execute low-level communication functions, thereby

providing useful abstractions to the communication software 2710. In an example embodiment, the interface station computer 304 is connected to the network 2724 using a modem, and the communication protocol layer 2714 is a dialup software module.

As shown, the interface station computer 304 may also contain one or more communication drivers 2712. Although multiple drivers may, in fact, be employed, for simplicity of discussion, the description hereinafter may refer to all such drivers as a single "driver." The communication driver 2712 acts both as a device driver for the interface unit 302, and also as a communications driver capable of accessing internet settings 2722 and facilitating communications between the Pocket Vault 102 and the server 114 by using the communication protocol layer 2714 to establish a connection to the network server 114 through the network 2724.

The network server 114 may comprise any suitable processor-based device or its equivalent. It may be either a single or multi-processor machine, or even a collection of servers inter-networked together. In one embodiment, the network server 114 stores both data and applications that are accessible to users. The network server 114 may, for example, store and serve a website, i.e., a collection of web pages and data that are available to users via a browser.

The network server 114 may include one or more controllers 402 and a database 406, as described above in connection with Figure 4. In addition, the network server 114 may include a communication protocol layer 2716, which provides low-level communication functions to server communications software. The communication protocol layer 2716 may be, but need not be, the same as the communication protocol layer 2714 of the interface station computer 304.

As shown in Fig. 27, the network server 114 may communicate through the network 2724 with an issuer authority 2718. The issuer authority 2718 may correspond, for example, to any of the advertiser(s) 108, non-financial media issuer(s) 110, or financial media issuer(s) 112 described above in connection with Fig. 1, or may be any entity designated to represent any of the same.

Overall, the networking arrangement illustrated in Fig. 27 allows the Pocket Vault 102 to access the network server 114. It also allows the interface station computer 304 to access restricted portions of the network server 114, such as, for example, user data stored in the database 406, when access is authenticated through communication from the Pocket Vault

102 to the network server 114. Authentication and access to restricted areas of the network server 114 will be further described below.

In order for the Pocket Vault 102 to perform communications functions, as well as other functions described elsewhere herein, the Pocket Vault 102 may be driven by control software 2708. Fig. 28 is a block diagram illustrating example components of the control software 2708 that may be disposed on the Pocket Vault 102.

As shown, the control software 2708 may include components such as a communications software module 2802, a card loading module 2804, an internet settings management module 2806, a synchronization module 2808, a statistics module 2810, and a security module 2812. It should be appreciated, of course, that the control software 2708 is not limited to the illustrative modules shown, and that the control software 2708 may comprise fewer modules or additional modules to perform other functions, such as the functionality described above in connection with Figs. 7-12.

The communications software module 2802 may, for example, be responsible for communications with the network server 114 and with the interface station computer 304, in the manner discussed below.

The card loading module 2804 may, for example, be responsible for loading data for new cards or tokens and storing such data in memory, as well as for transferring this data to the network server 114, when appropriate. Examples of how card/token data may be loaded onto the Pocket Vault 102 are discussed below in connection with Fig. 34.

Internet settings management module 2806 may, for example, be responsible for managing the storage and use of internet settings by the Pocket Vault 102. Such internet settings may, for example, correspond to any of the internet settings 2722 that may be stored on the interface station computer 304. The internet settings management module 2806 may allow a user to store, manage, and transfer internet settings, e.g., cookies and preference settings, from one computer to another. Operation of the internet settings management module 2708 will be further described below in connection with the steps 3310 and 3320 of the routine 3024 (Fig. 33).

The synchronization module 2808 may, for example, be responsible for synchronizing data and settings stored on the Pocket Vault 102 with data and settings stored on the network server 114. Operation of the synchronization module 2808 is described below in connection with Fig. 35.

The statistics module 2810 may, for example, collect statistics concerning use of the Pocket Vault 102. Such statistics may, for example, include information such as the number of accesses to various cards stored in the memory of the Pocket Vault 102, the number of financial transactions engaged in, the date of the last update of the Pocket Vault 102, the total amount and kind of data transferred between the Pocket Vault 102 and each interface station 104 and/or the network server 114. In addition, the statistics module 2810 may be adapted to be customized by the user.

The security module 2812 may, for example, ensure security of authentication and communications. All communications to and from the network server 114 and the interface station 104 may be encrypted by the security module 2812, so that any attacker who intercepts those communications will receive no useful information.

Any of numerous types of encryption may be used to satisfactorily protect communications between the Pocket Vault 102 and the other devices in the network. For example, one of the asymmetric-key encryption types, such as public key encryption or private key encryption, may be used. These public/private encryption techniques are well known in the art and therefore will not be described here in detail. Alternatively, one-time pad encryption or other encryption techniques may be used to achieve a similar objective.

As discussed above, the Pocket Vault 102 may be adapted to not release any personal or secure information, even encrypted, until the holder presents satisfactory verification of his or her identity, such as, for example, presenting the holder's fingerprint to the fingerprint scanner 220 or entering a password. In addition, fingerprint and password protection may be used together for authentication purposes, such that personal or secure information can be transferred or released only if the holder has been successfully authenticated using both techniques.

In alternative embodiments, security may be implemented using different measures, or may be omitted altogether in situations where the interface station computer 304 is a trusted host. In addition, security module 2812 may be called on to perform security functions in situations other than communicating with the network server 114 and the interface station computer 304.

The manner of communication among the Pocket Vault 102, the network server 114, and an interface station computer 304 will now be described in connection with Figure 29. Figure 29 is a data flow diagram illustrating how data may be transferred between the Pocket

Vault 102 and a user interface 2902 of the interface station computer 304. The user interface 2902 may, for example, comprise a web browser included in the communications software 2710 running on the interface station computer 304. Alternatively, it may be a stand-alone application that allows a user to interact with the communications software 2710 and, through it, interact with a website located on the network server 114.

In the illustrative embodiment shown, the data transfer takes place via the communication driver 2712, the network server 114, and the communications software 2710, data can flow in both directions at all connection points, and all communications between the Pocket Vault 102 and the user interface 2902 of the interface station computer 304 pass through the network server 114.

Using the arrangement shown, the user may, for example, update settings on the Pocket Vault 102 by using the user interface 2902 and the communication software 2710 to update settings on the network server 114, and then instructing the network server 114 to update settings on the Pocket Vault 102 via the communication driver 2712.

In one embodiment, the network server 114 implements a website, where user information may be selectively stored and accessed by a person using the communication software 2710 (e.g., a web browser) running on the interface station computer 304, and any user may access the website on the network server 114. However, the website may have a so-called "restricted area" which can be accessed only after the user has authenticated his or her identity. As used herein, the term "restricted area" or "restricted information" means any data that is not available to general public without some sort of authentication. For example, each user may have preferences stored in the database 406 that would indicate how the main site should be presented to that user. Those preferences will not be available to other users. In addition to such relatively low-security settings, such as website preferences, database 406 may also contain private user information, such as information about a user's credit cards and identity information. Access to this restricted information may be limited, for example, to only "authenticated" users.

Authentication of a Pocket Vault holder may be achieved, for example, by the holder applying a fingerprint to the fingerprint scanner 220 of the Pocket Vault 102, interfacing the Pocket Vault 102 with the interface unit 302 (which acts essentially as a pass-through device), and establishing a connection between the Pocket Vault 102 and the network server 114 via the communication driver 2712. Based on communications with the Pocket Vault

102 via this "connection," the website may determine: (1) whether the Pocket Vault 102 has been "validated," i.e., whether a fingerprint has been stored in the fingerprint memory of the Pocket Vault 102 and whether validation information (e.g., a PKI certificate) is present on the Pocket Vault 102, and (2) whether the Pocket Vault 102 has been authenticated, i.e., whether the fingerprint recently scanned by the Pocket Vault 102 matched the fingerprint stored in the fingerprint memory of the Pocket Vault 102. If the website determines that the Pocket Vault 102 has not yet been validated, the user may be given an option to validate the Pocket Vault 102 using the website software. If the website determines that the Pocket Vault 102 has been validated and authenticated, then the network server 114 may enable the authenticated holder to access or perform functions relating to some or all of the restricted area of the database 406 containing that holder's information.

Communication driver 2712 may be a light-weight application that can access and modify the internet settings 2722, and can also access communications protocol layer 2714, but cannot transfer information to any other software programs. For example, the communication driver 2712 may access the internet settings 2722 in order to determine that the interface station computer 304 is connected to the network 2724 through a dial-up connection; following that, it may initiate the dial-up connection or use an established connection through the communications protocol layer 2714 in order to tunnel packets from the Pocket Vault 102 to the network 2724.

Fig. 30 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO ACCESS WEBSITE routine 1422 shown in Fig. 14, which may be executed by the controller 308 of the interface station computer 304. As discussed above in connection with Fig. 14, it should be appreciated that this routine need not be accessed as a result of a user selecting it from the menu displayed in the step 1402. Rather, a user may simply use a browser to directly log onto the website on the network server 114.

As shown, the routine 1422 begins at a step 3002, wherein the interface station computer 304 is caused to access the website on the network server 114, e.g., by using a browser to access the website.

After the step 3002, the routine 1422 proceeds to a step 3004, wherein it is determined whether the requisite communication drivers 2712 have been installed.

When, at the step 3004, it is determined that the requisite communication drivers 2712 have not been installed, the routine 1422 proceeds to an INSTALL DRIVER(S) routine 3006

(discussed below in connection with Fig. 31), which is responsible for installing the communication drivers 2712.

After the routine 3006 has completed, the routine 1422 proceeds to a step 3008, wherein the communication drivers 2712 are caused to become operational.

When, at the step 3004, it is determined that the requisite drivers 2712 have already been installed, the routine 1422 proceeds directly to the step 3008 (discussed above).

After the step 3008, the routine 1422 proceeds to steps 3010-3016, wherein attempts are made to establish a connection between the Pocket Vault 102 and the website on the network server 114 within a time out period determined by the step 3014. Each time it is determined that the connection has not yet been established, the user is prompted to interface the Pocket Vault 102 with the interface unit 302 and to connect the interface unit 302 to the interface station computer 304 (e.g., using a USB cable).

When, during the steps 3010-3016, it is determined that a connection has not been established between the Pocket Vault 102 and the website in a timely manner, the routine 1422 proceeds to a step 3026, wherein a message is displayed to the user regarding the unsuccessful communication attempt between the Pocket Vault 102 and the website on the network server 114.

After the step 3026, the routine 1422 terminates.

When, during the steps 3010-3016, it is determined that a connection has been successfully established between the Pocket Vault 102 and the website on the network server 114, the routine 1422 proceeds to a step 3018, wherein it is determined whether the Pocket Vault 102 has been validated, e.g., whether a holder's fingerprints and a PKI certificate are stored therein. The website may, for example, make this determination based upon the messages exchanged during the handshaking protocol engaged in between the Pocket Vault 102 and the network server 114.

When, at the step 3018, it is determined that the Pocket Vault 102 has not yet been validated, the routine 1422 proceeds to a NEW POCKET VAULT HOLDER routine 3020, which is discussed below in connection with Fig. 32.

When, at the step 3018, it is determined that the Pocket Vault 102 has already been validated, the routine 1422 proceeds to an EXISTING POCKET VAULT HOLDER routine 3024, which is discussed below in connection with Fig. 33.

After completion of the EXISTING POCKET VAULT HOLDER routine 3024, the routine 1422 terminates.

After completion of the NEW POCKET VAULT HOLDER routine 3020, the routine 1422 proceeds to a step 3022, wherein it is determined whether a new holder was successfully validated.

When, at the step 3022, it is determined that a new holder was successfully validated, the routine 1422 proceeds to the EXISTING POCKET VAULT HOLDER routine 3024 (discussed above).

When, at the step 3022, it is determined that a new holder was not successfully validated, the routine 1422 terminates.

Fig. 31 is a flow diagram illustrating an example implementation of the INSTALL DRIVER(S) routine 3006 shown in Fig. 30.

As shown, the routine 3006 begins at a step 3102, wherein the necessary communication drivers 2712 are downloaded from another computer, e.g., a website on the World Wide Web.

After the step 3102, the routine 3006 proceeds to steps 3104-3108, wherein the necessary communication drivers 2712 are installed on the interface station computer 304 and registered with network server 114, and the preferences for the communication drivers 2712 are set either automatically or in response to user input. During the step 3106, the communication driver 2712 may communicate with the network server 114 in order to register itself and its attributes. Among these attributes can be such things as a unique identifier for the interface station computer 304 on which that driver is installed, the identity of the user registering it, and other such items. The preferences that may be set by the user during the step 3108 may, for example, include information such as how and where to access the internet settings 2722, how many attempts at connection should be performed, etc.

After the step 3108, the routine 3006 terminates.

Fig. 32 is a flow diagram illustrating an example implementation of the NEW POCKET VAULT HOLDER routine 3020 shown in Fig. 30.

As shown, the routine 3020 begins at a step 3202, wherein it is determined whether the new holder has indicated that he or she has already established an account with the website on the network server 114.

When, at the step 3202, it is determined that the new holder has not indicated the existence of a previously-established account, the routine 3020 proceeds to a step 3204, wherein a new account is established on the website on the network server 114 in response to user input to a browser running on the interface station computer 304.

After the step 3204, the routine 3020 proceeds to a step 3206, wherein the new holder is prompted to apply his or her fingerprint to the fingerprint scanner 220 while the Pocket Vault 102 is interfaced with the interface unit 302. The user is further prompted to follow the directions on the Pocket Vault 102. As discussed above in connection with Figs. 7 and 8, when a fingerprint is applied to a fingerprint scanner 220 of an un-validated device, the user is instructed by the Pocket Vault to apply six finger prints (three from one finger on the left hand and three from one finger on the right hand) sequentially to the fingerprint scanner 220, waiting for a beep each time. As discussed in connection with Fig. 8, after the new holder has completed this task, an encrypted message including the Pocket Vault ID may be released from the Pocket Vault to the interface unit 302. Because of the established connection between the Pocket Vault 102 and the website on the network server 114, this encrypted message should reach the website. And, in response to receiving this encrypted message, the website should release encrypted validation information (e.g., a PKI certificate) back to the Pocket Vault 102 via the established connection.

After the step 3206, the routine 3020 proceeds to steps 3208-3210, wherein it is determined whether the Pocket Vault 102 has released the encrypted message including the Pocket Vault ID to the website before a timeout period has elapsed.

When, at the step 3210, it is determined that the timeout period elapsed before the encrypted message including the Pocket Vault ID was released to the website, the routine 3020 proceeds to a step 3220, wherein a message is displayed to the user concerning the unsuccessful attempt to validate the Pocket Vault holder.

After the step 3220, the routine 3020 terminates.

When, at the steps 3208-3210, it is determined the Pocket Vault 102 has released the encrypted message including the Pocket Vault ID to the website before the timeout period elapsed, the routine 3020 proceeds to a step 3212, wherein it is determined whether the website has released the encrypted validation information (e.g., a PKI Certificate) to the Pocket Vault 102.

When, at the step 3210, it is determined that the timeout period elapsed before the website released the encrypted validation information (e.g., a PKI Certificate) to the Pocket Vault 102, the routine 3020 proceeds to the step 3220 (discussed above).

When, at the step 3210, it is determined that the website released the encrypted validation information (e.g., a PKI Certificate) to the Pocket Vault 102 before the timeout period elapsed, the routine 3020 proceeds to a step 3216, wherein a message is displayed to the user concerning the successful validation of the new Pocket Vault holder.

After the step 3216, the routine 3020 terminates.

When, at the step 3202, it is determined that the new holder has indicated the existence of a previously-established account, the routine 3020 proceeds to a step 3218, wherein a check is made to verify the holder's identity. The holder may, for example, be required to enter personal information, such as name, contact information, and security information to verify his or her identity.

When, at the step 3218, it is determined that the holder has successfully verified his or her identity, the routine 3020 proceeds to the step 3206 (discussed above), with the holder's previously-stored account information being used for the new Pocket Vault 102.

When, at the step 3218, it is determined that the holder has not successfully verified his or her identity, the routine 3020 proceeds to the step 3220 (discussed above).

Fig. 33 is a flow diagram illustrating an example implementation of the EXISTING POCKET VAULT HOLDER routine 3024 shown in Fig. 30.

As shown, the routine 3024 begins at a step 3302, wherein it is determined whether the Pocket Vault 102 has been authenticated, e.g., whether the Pocket Vault 102 has determined that a fingerprint applied to the fingerprint scanner 220 matches one of the fingerprints stored in the fingerprint memory of the Pocket Vault 102. This authentication procedure may operate as described above in connection with the step 712 (Fig. 7), or an additional or different routine may be employed (e.g., as part of the security module 2812 described above in connection with Fig. 28) to determine whether the holder has successfully authenticated his or her identity, thereby enabling the network server 114 to establish a "trust" relationship with the Pocket Vault 102.

When, at the step 3302, it is determined that the Pocket Vault 102 has not been properly authenticated, the routine 3024 proceeds to a step 3304, wherein the holder is prompted to apply his or her fingerprint to the fingerprint scanner 220 of the Pocket Vault

102 while the Pocket Vault 102 is interfaced with the interface unit 302, i.e., while keeping the connection established between the Pocket Vault 102 and the website on the network server 114.

As shown, the step 3306 determines whether the Pocket Vault 102 has been properly authenticated prior to the expiration of a timeout period.

When, at the step 3306, it is determined that the timeout period elapsed before the Pocket Vault 102 was authenticated, the routine 3024 proceeds to a step 3308, wherein a message is displayed indicating that the authentication attempt was unsuccessful.

After the step 3308, the routine 3024 terminates.

When, at the step 3302, it is determined that the Pocket Vault 102 has been properly authenticated, the routine 3024 proceeds to a step 3310, wherein the communication driver 2712 causes the internet settings 2722 of the interface station computer 304 to be adjusted to reflect certain internet settings stored in the Pocket Vault 102, e.g., by the internet settings management module 2806. In this manner, the internet settings of the Pocket Vault 102 may be "ported" to the interface station computer 304 so that the browser operating on the interface station computer 304 may take advantage of those settings while the Pocket Vault 102 is connected to the website on the network server 114 via the communication driver 2712. The internet settings of the Pocket Vault 102 that may be ported to the interface station computer 304 in this manner may comprise, for example, the network name and identification of the Pocket Vault 102, an identification of communications protocols used to connect to the network 2724, network preferences, such as whether any proxy servers may or should be used, a list of frequently-used servers, cookies previously obtained from various websites, digital certificates, personal bookmarks, user identity data, user password data for various servers, etc.

The internet settings on the Pocket Vault 102, and porting of the same to the interface station computer 304, may be managed, for example, by one or more modules of the control software, e.g., the internet settings management module 2806. In one embodiment, the user may elect which internet settings are to be ported to the interface station computer 304 during the step 3310. This functionality may be accomplished, for example, during a SET PREFERENCES routine 3324 (described below in connection with Fig. 39).

After the step 3310, the routine 3024 proceeds to a step 3312, wherein it is determined whether one of several "functions" has been selected. In the illustrative embodiment shown,

the seven available functions are: (1) CARD LOADING (see CARD LOADING routine 3314 -- discussed below in connection with Fig. 34), (2) SYNCHRONIZATION (see SYNCHRONIZATION routine 3316 -- discussed below in connection with Fig. 35), (3) RECOVERY (see RECOVERY routine 3318 -- discussed below in connection with Fig. 36), (4) IDENTITY PORTING OPTIONS (see IDENTITY PORTING OPTIONS routine 3320 -- discussed below in connection with Fig. 337), (5) BACKUP (see BACKUP routine 3322 -- discussed below in connection with Fig. 38), (6) SET PREFERENCES (see SET PREFERENCES routine 3324 -- discussed below in connection with Fig. 39), AND (7) TERMINATE SESSION (see step 3326). It should be appreciated that the invention is not limited to the specific functions shown, and that additional, different or fewer functions may be employed.

It should further be appreciated that some or all of the illustrated functions, or operations relating to such functions, may be initiated automatically or may require user initiation, depending on the setting of preferences. For example, the SYNCHRONIZATION routine 3316 may be initiated automatically after completion of the step 3310, if preferences so indicate. Alternatively, certain steps required to accomplish synchronization of the Pocket Vault 102 and the website on the network server 114 may be taken, without actually completing the synchronization. For example, the synchronization module 2808 of the control software 2708 may automatically initiate a comparison of the contents of the Pocket Vault 102 and the website to determine what data should be transferred if synchronization is initiated. Software on the network server 114 may also or alternatively perform a similar comparison function automatically, if so desired.

Moreover, it should be understood that, in some embodiments, some of the above-noted functions may be performed without first requiring a Pocket Vault 102 to be authenticated. For example, some functions may involve the transfer of public or non-sensitive data, and may not require protection via the authentication verification step 3302.

As shown in Fig. 33, when any of the above-listed seven functions is selected, either automatically or in response to user input, the selected function is performed. For each of functions 3314, 3316, 3318, 3320, 3322, and 3324, after performing the routine associated with the function, the routine 3024 proceeds to a step 3332, wherein it is determined whether the connection between the Pocket Vault 102 and the website on the network server 114 is still established.

When, at the step 3332, it is determined that the connection between the Pocket Vault 102 and the website on the network server 114 is still established, the routine 3024 returns to the step 3312 (discussed above).

When, at the step 3332, it is determined that the connection between the Pocket Vault 102 and the website on the network server 114 is no longer established, the routine 3024 proceeds to a step 3327, wherein some or all of the internet settings 2722 are ported from the interface station computer 304 to the Pocket Vault 102. The communication driver 3712 may cause the settings to be ported directly to the Pocket Vault 102 from the interface station computer 304 (via the interface unit 302), or the settings may be transferred first to the network server 114 and then to the Pocket Vault 102 (via the connection between the network server 114 and the Pocket Vault 102). In some embodiments, only certain types or classes of settings, e.g., certain type of cookies, PKI certificates, etc., are ported from the interface station computer 304 to the Pocket Vault 102 in this manner. The classes or types of settings that are ported during the step 3327 may, for example, be determined by the user in some embodiments. For example, the user may set certain preferences, e.g., during the SET PREFERENCES routine 3324 or by manipulating the Pocket Vault 102 directly, that control the nature and type of internet settings that are ported to the Pocket Vault 102 from the interface station computer 304 during the step 3327.

After the step 3327, the routine 3024 proceeds to a step 3328, wherein the communication driver 2712 causes the internet settings 2722 on the interface station computer 304 to return to their original state, i.e., the configuration the internet settings 2712 were in before they were altered in the step 3310.

After the step 3328, the routine 3024 proceeds to a step 3330, wherein any cached web pages or other information temporarily stored in the interface station computer 304 during the communication session between the Pocket Vault 102 and the website on the network server 114 are deleted from cache and other memory in the interface station computer 304. Thus, after completion of the step 3330, the interface station computer 304 is in essentially the same state it was in prior to the beginning of the routine 1422. The communication driver 2712 may remain on the interface station computer 304 or may be deleted in connection with the step 3330. If the communication driver 2712 is kept on the interface station computer 304, any cache or other memory associated with it that might store personal or sensitive information may also be erased. In some embodiments, the

communication driver 2712 caches or stores very little, if any, information that is passed between the Pocket Vault 102 and the website on the network server 114. In any event, the communication driver 2712 may be constructed such that no useful data, i.e., data that reflects any personal or sensitive information, remains on it after completion of the step 3330.

When, at the step 3312, the holder chooses the TERMINATE SESSION function, the connection between the Pocket Vault 102 and the website on the network server 114 is de-established, and the routine 3024 proceeds immediately to the steps 3327, 3328 and 3330 (discussed above).

After the step 3330, the routine 3024 terminates.

Fig. 34 is a flow diagram illustrating an example implementation of the CARD LOADING routine 3314 shown in Fig. 33.

As shown, the routine 3314 begins at a step 3402, wherein a determination is made as to whether the card desired to be loaded is "swipeable." The user may, for example, be prompted to indicate whether the card has an operational magnetic stripe disposed thereon.

When, at the step 3402, the user indicates that the card does not have an operational magnetic stripe, the routine 3314 proceeds to a step 3406, wherein the user is prompted (e.g., via the browser on the interface station computer 304) to input information to be used in creating a card account.

When, at the step 3402, the user indicates that the card does have an operational magnetic stripe, the routine 3314 proceeds to the step 3410, wherein the user is prompted to swipe the card through the stripe reader 315 of the interface unit 302.

After the step 3406, the routine 3314 proceeds to steps 3408 and 3409, wherein it is determined whether the interface station computer 304 has received the information from a card swiped through the stripe reader 315 of the interface unit 302 prior to the expiration of a timeout period.

When, at the step 3409, it is determined that the timeout period elapsed before information from a swiped card was received, the routine 3314 proceeds to a step 3411, wherein a message is displayed to the user concerning the failure to properly read the magnetic stripe.

After the step 3411, the routine 3314 returns to the step 3402 (discussed above). Thus, when a user is unsuccessful in swiping a card one or more times, the user may determine that the magnetic stripe is non-operational, and may indicate at the step 3402 that

the card is not swipeable. The user may thereafter create an account for the card manually at the step 3410 (discussed above).

After the step 3410, the routine proceeds to a step 3412, wherein the website on the network server 114 determines whether the account for the card is valid. This determination may be made, for example, by confirming that the card is owned by the person attempting to add it to his or her Pocket Vault 102, that the card has not expired, etc.

When, at the step 3408, it is determined that information from the swiped card has been received prior to the expiration of the timeout period, the routine 3314 proceeds to the step 3412 (discussed above), wherein a determination is made as the validity of the account based upon the information read by the stripe reader 315.

When, at the step 3412, a determination is made that the account the user has requested to be added to the Pocket Vault 102 is not valid, the routine 3314 proceeds to a step 3414 wherein appropriate security precautions are taken.

After the step 3414, the routine 3314 terminates.

When, at the step 3412, a determination is made that the account the user has requested to be added to the Pocket Vault 102 is valid, the routine 3314 proceeds to a step 3416, wherein the information for the card is downloaded from the website on the network server 114 to the Pocket Vault 102 via the communication driver 2712.

After the step 3416, the routine 3314 proceeds to a step 3418, wherein a message is displayed that indicates the card has been successfully loaded onto the Pocket Vault 102 for use in future transactions.

After the step 3418, the routine 3314 terminates.

Fig. 35 is a flow diagram illustrating an example implementation of the SYNCHRONIZATION routine 3316 shown in Fig. 33.

As shown, the routine 3316 begins at a step 3502, wherein certain parameters required to synchronize the Pocket Vault 102 to the website on the network server 114 are determined based upon user preferences and the ID of the Pocket Vault 102. For example, if a holder has two or more Pocket Vaults 102, the holder may wish to elect one of them to be a master for synchronization purposes, or the holder may even elect to have the website act as the master. When a holder has more than one Pocket Vault 102, the holder also may desire to be prompted to select either the current date or the date of the last synchronization as the basis for the synchronization operation.

After the step 3502, the routine 3316 proceeds to a step 3504, wherein the website on the network server 114 generates sets of current data to transfer to the Pocket Vault 102. The website may, for example, compare its current data to the data stored on the Pocket Vault 102 so as to identify any data it needs to receive from the Pocket Vault 102 to properly synchronize therewith.

After the step 3504, the routine 3316 proceeds to steps 3506 and 3508, wherein it is determined whether the Pocket Vault 102 has indicated that it is ready to synchronize prior the expiration of a timeout period (measured by the step 3508). The Pocket Vault 102 may, for example, also be performing a similar comparison (e.g., using the synchronization module 2808) between its data and the data stored on the website of the network server to determine what data it needs to receive from the website to properly synchronize therewith.

When at the step 3508, it is determined that the timeout period has elapsed before the Pocket Vault 102 had indicated its readiness to synchronize, the routine 3316 proceeds to a step 3510, wherein a message is generated indicating the attempt to synchronize the Pocket Vault 102 with the website on the network server 114 has failed.

After the step 3510, the routine 3316 terminates.

When at the step 3506, it is determined that the Pocket Vault 102 has indicated its readiness to synchronize with the website prior to the expiration of the timeout period, the routine 3316 proceeds to a step 3512, wherein accumulated synchronization data is transferred from the website to the Pocket Vault 102, and vice versa, via the communication driver 2712.

After the step 3512, the routine 3316 proceeds to a step 3516, wherein the date of the successful synchronization is stored in both the Pocket Vault 102 and the network server 114.

After the step 3516, the routine 3316 proceeds to a step 3518, wherein a message is generated indicating that the Pocket Vault 102 has been successfully synchronized with the website on the network server 114.

After the step 3518, the routine 3316 terminates.

Figure 36 is a flow diagram illustrating an example implementation of the RECOVERY routine 3318 shown in Fig. 33.

As shown, the routine 3318 begins at a step 3602, wherein the website on the network server 114 compiles all data necessary to recover the Pocket Vault 102 to its state as of the last time its contents were synchronized with the website of the network server 114 (e.g.,

using the routine 3316 – described above) or backed up on the website of the network server 114 (e.g., using routine 3322 – described below).

After the step 3602, the routine 3318 proceeds to step 3604, wherein the data compile in the step 3602 is downloaded from the website on the network server 114 to the Pocket Vault 102 via the communication driver 2712, and a determination is made as to where that downloading has completed prior to the expiration of a timeout period measured at the step 3606.

When, at the step 3606, it is determined that the timeout period elapsed prior to the downloading being completed, the routine 3318 proceeds to a step 3608, wherein a message is generated indicating that the attempted recovery was unsuccessful.

After the step 3606, the routine 3318 terminates.

When, at the step 3606, it is determined that the downloading was completed in a timely manner, the routine 3318 proceeds to a step 3610, wherein a message is generated indicating that the attempted recovery of data to the Pocket Vault 102 was successful.

After the step 3610, the routine 3318 terminates.

Figure 37 is a flow diagram illustrating an example implementation of the IDENTITY PORTING SELECTION routine 3320 shown in Fig. 33.

As shown, the routine 3320 begins at a step 3702, wherein the internet settings 2722 from the interface station computer 304 are downloaded from the interface station computer 304 to the website on the network server 114.

After the step 3702, the routine 3320 proceeds to a step 3704, wherein the website on the network server 114 compiles and displays the downloaded internet settings to the user via the browser on the interface station computer 304. The settings may be displayed to the user in any of a number of ways. Preferably, the settings are displayed in a manner that enables the user to readily distinguish between various classes of settings, and that permits the user to readily identify the purpose of each type of setting. In some embodiments, only a subset of the all of the internet settings 2722 (e.g., only settings such as cookies and PKI certificates) are transferred to the website for possible modification by the user.

After the step 3704, the routine 3320 proceeds to steps 3706 and 3708, wherein the user is given an opportunity to modify the displayed internet settings. The user may, for example, elect to keep certain cookies that were retained among the internet settings 2722, while choosing to discard others.

When at the step 3708, the user has indicated that he or she has completed any modifications of the retrieved internet settings 2722, the routine 3320 proceeds to a step 3710, wherein the modified internet settings are downloaded from the website on the network server 114 to the Pocket Vault 102 via the communication driver 2712.

After the step 3710, the routine 3320 terminates.

When at the step 3706, it is determined that the user did not elect to modify any settings, the routine 3320 terminates.

Figure 38 is a flow diagram illustrating an example implementation of the BACKUP routine 3322 shown in Fig. 33.

As shown, the routine 3322 begins at a step 3802, wherein the website on the network server 114 transmits a request to the Pocket Vault 102 via the communication driver 2712, asking the Pocket Vault 102 to send the website backup data. This backup data may, for example, constitute all data necessary to place the Pocket Vault 102 back into its present state if any portion of data on the Pocket Vault 102 was lost, or to place a new Pocket Vault 102 into the same state as the backed up Pocket Vault 102 (e.g., using the RECOVERY routine 3318 – discussed above).

After the step 3802, the routine 3322 proceeds to steps 3804 -3806, wherein it is determined whether the requested backup data has been successfully transferred from the Pocket Vault 102 to the website on the network server 114 before the expiration of a timeout period (measured by the step 3806).

When, at the step 3806, it is determined that the timeout period elapsed prior to the backup data being successfully transferred, the routine 3322 proceeds to a step 3808, wherein a message is displayed (e.g., via the browser on the interface station computer 304) informing the user that a communication error has occurred and that the backup operation was unsuccessful.

After the step 3808, the routine 3322 terminates.

When, at the step 3804, the routine 3322 determined that, before the timeout period, the backup data has been successfully transferred from the Pocket Vault 102 to the website on the network server 114 via the communication driver 2712, the routine 3322 proceeds to a step 3810, wherein the received backup data is stored by the network server 114, e.g., for use in connection with the RECOVERY routine 3318.

After the step 3310, the routine 3322 proceeds to a step 3812, wherein a message is displayed (e.g., via the browser on the interface station computer 304) informing the user that the backup operation was successfully completed.

After the step 3312, the routine 3322 terminates.

Figure 39 is a flow diagram illustrating an example implementation of the SET PREFERENCES routine 3324 shown in Fig. 33. The SET PREFERENCES routine 3324 permits the holder to set or alter preferences on his or her Pocket Vault 102 using a browser on the interface station computer 104.

As shown, the routine 3324 begins at a step 3902, wherein the website on the network server 114 transmits a request to the Pocket Vault 102 via the communication driver 2712, requesting the Pocket Vault 102 to transmit all "preferences" information stored on the Pocket Vault 102 to the website on the network server 114 via the communication driver 2712. This information may, for example, comprise definitions of home pages, connection of secure and non-secure media, order of media presentment, sort orders, user interface options, synchronization defaults, etc.

After the step 3902, the routine 3324 proceeds to steps 3904 and 3906, wherein it is determined whether the preferences information has been received from the Pocket Vault 102 prior to the expiration of a timeout period (measured by the step 3906).

When, at the step 3906, it is determined that the timeout period elapsed before the preferences information was transferred from the Pocket Vault 102 to the website, the routine 3324 proceeds to a step 3908, wherein a message is displayed (e.g., on the browser) indicating that a communication error has occurred.

After the step 3908, the routine 3324 terminates.

When, at the step 3904, it is determined that the preferences information has been successfully transferred from the Pocket Vault 102 to the website on the network server 114, the routine 3324 proceeds to a step 3910, wherein the website compiles and displays the current preference settings for the Pocket Vault 102 (e.g., on the browser) in a user friendly manner.

After the step 3910, the routine 3324 proceeds to steps 3912 and 3914, wherein the user is given an opportunity to modify the displayed preference settings.

When, at the step 3912, the user opts not to modify any of the displayed settings, the routine 3324 terminates.

When, at the steps 3912 and 3914, the user opts to modify the displayed settings and indicates that he or she has completed modification thereof, the routine 3324 proceeds to a step 3916, wherein the modified preference settings are downloaded from the website on the network server 114 to the Pocket Vault 102 via the communication driver 2712.

After the step 3918, a message is displayed (e.g., via the browser on the interface station computer 304) informing the user that the preference settings for the Pocket Vault 102 were successfully modified.

After the step 3918, the routine 3324 terminates.

One illustrative example of an application of the network system described herein is in the distribution of building access key cards and similar limited-use, time-sensitive media to individual operators. The following typical scenario involves distribution of hotel room key cards to hotel guests who make room reservations over the Internet. Using a hotel's secure web site, the prospective guest, who is also a Pocket Vault holder, may secure a room for a specific time period by providing a credit card number. This step may or may not involve use of a credit card stored on the Pocket Vault 102. If it does involve use of a Pocket Vault credit card, this card may, for example, be accessed while the Pocket Vault 102 is interfaced with the holder's personal interface station 104b. Next, the prospective hotel guest may link to the network server 114 (while staying within the hotel's website), and follow on-screen instructions for downloading the key card for his/her room onto the Pocket Vault 102 (e.g., to ensure that the Pocket Vault 102 is interfaced with the pocket vault interface unit 302, and to ensure that the Pocket Vault holder has activated the Pocket Vault 102 by the appropriate security mechanism such as a thumbprint for bio-metric ID verification). After downloading is complete, the display 216 of the Pocket Vault 102 may include an icon for the hotel room key (e.g., the hotel's logo), along with the icons for media previously loaded. When the room key card icon is selected, the Pocket Vault 102 may encode the Chameleon Card with the magnetic stripe coding to unlock the guest's hotel room.

After the time period of the guest's room reservation has expired, the Pocket Vault 102 may automatically delete the room key icon. This deletion may occur for the convenience of the Pocket Vault holder, not necessarily for hotel security reasons, since the room's lock will reject any previously-used key card (Chameleon or traditional key card) after the key card's specified time period has expired.

Having thus described at least one illustrative embodiment of the invention, various alterations, modifications and improvements will readily occur to those skilled in the art. Such alterations, modifications and improvements are intended to be within the spirit and scope of the invention. Accordingly, the foregoing description is by way of example only and is not intended as limiting. The invention is limited only as defined in the following claims and the equivalents thereto.

What is claimed is:

CLAIMS

1. A method for enabling a software module on a computer operated by a user to access restricted information on a server, comprising steps of:

(A) with an electronic device distinct from the computer, authenticating an identity of the user to determine that the user is permitted to access the restricted information on the server; and

(B) in response to the electronic device authenticating the identity of the user operating the computer, enabling the software module on the computer to access the restricted information on the server.

2. The method of claim 1, wherein the step (A) comprises comparing, with the electronic device, a measured bio-metric parameter of the user with a stored bio-metric parameter of the user.

3. The method of claim 1, further comprising a step of:

(C) accessing, with the software module on the computer, the restricted information on the server.

4. The method of claim 3, further comprising a step of:

(D) establishing a connection between the electronic device and the server.

5. The method of claim 4, wherein the step (D) includes establishing the connection via a driver in the computer.

6. The method of claim 4, further comprising steps of:

(D) in response to input to the computer by the user, altering settings stored on the server; and

(E) transmitting a signal from the server to the electronic device via the connection, the signal causing the settings on the electronic device to be changed to correspond to the altered settings stored on the server.

7. The method of claim 1, further comprising a step of:

(C) transmitting a signal from the computer to the server, which signal indicates that the electronic device has authenticated the identity of the user of the computer and determined that the user is permitted to access the restricted information on the server.

8. A method for altering settings on a computer to correspond to settings on an electronic device distinct from the computer, comprising steps of:

(A) with the electronic device, authenticating an identity of a user to determine that the user is authorized to use the electronic device; and

(B) in response to authenticating the identity of the user to determine that the user is authorized to use the electronic device, altering the settings on the computer to correspond to settings on the electronic device.

9. The method of claim 8, further comprising a step of:

(C) with the computer, accessing a server based upon the settings on the computer.

10. The method of claim 9, further comprising a step of:

(D) establishing a connection between the electronic device and the server.

11. The method of claim 10, wherein the step (D) includes establishing the connection via a driver in the computer.

12. The method of claim 11, wherein the step (B) includes, using the driver to update the settings on the computer.

13. The method of claim 10, further comprising steps of:

(E) altering the settings on the computer in response to user input to the computer; and

(F) transferring at least some of the altered settings on the computer to the electronic device when the connection is de-established.

14. The method of claim 10, further comprising a step of:

(E) restoring the settings on the computer to their original state when the connection is de-established.

15. The method of claim 8, wherein the step (A) comprises comparing, with the electronic device, a measured bio-metric parameter of the user with a stored bio-metric parameter of the user.

16. The method of claim 8, wherein the settings comprise at least one of a bookmark list, a web site cookie, an encoding of a user password, and personal user data.

17. A system for enabling a software module on a computer operated by a user to access restricted information on a server, comprising:

an electronic device distinct from the computer, the electronic device including a user-authenticator to authenticate an identity of the user to determine that the user is permitted to access the restricted information on the server; and

means for, in response to the electronic device authenticating the identity of the user operating the computer, enabling the software module on the computer to access the restricted information on the server.

18. The system of claim 17, wherein the user authenticator includes a bio-metric authenticator.

19. The system of claim 17, further comprising:

means for accessing, with the software module on the computer, the restricted information on the server.

20. The system of claim 19, further comprising:

means for establishing a connection between the electronic device and the server.

21. The system of claim 19, further comprising:

means for, in response to input to the computer by the user, altering settings stored on the server; and

means for transmitting a signal from the server to the electronic device via the connection, the signal causing the settings on the electronic device to be changed to correspond to the altered settings stored on the server.

22. The method of claim 17, further comprising:

means for transmitting a signal from the computer to the server, which signal indicates that the electronic device has authenticated the identity of the user of the computer and determined that the user is permitted to access the restricted information on the server.

23. A system for altering settings on a computer to correspond to settings on an electronic device distinct from the computer, comprising:

a user authenticator included in the electronic device to authenticate an identity of a user to determine that the user is authorized to use the electronic device; and

means for, in response to authenticating the identity of the user to determine that the user is authorized to use the electronic device, altering the settings on the computer to correspond to settings on the electronic device.

24. The system of claim 23, further comprising:

means for accessing a server with the computer based upon the settings on the computer.

25. The system of claim 24, further comprising:

means for establishing a connection between the electronic device and the server.

26. The system of claim 25, further comprising:

means for altering the settings on the computer in response to user input to the computer; and

means for transferring at least some of the altered settings on the computer to the electronic device when the connection is de-established.

27. The system of claim 25, further comprising:

means for restoring the settings on the computer to their original state when the connection is de-established.

28. The system of claim 23, wherein the user authenticator includes a bio-metric authenticator.

29. The system of claim 23, wherein the settings comprise at least one of a bookmark list, a web site cookie, an encoding of a user password, and personal user data.

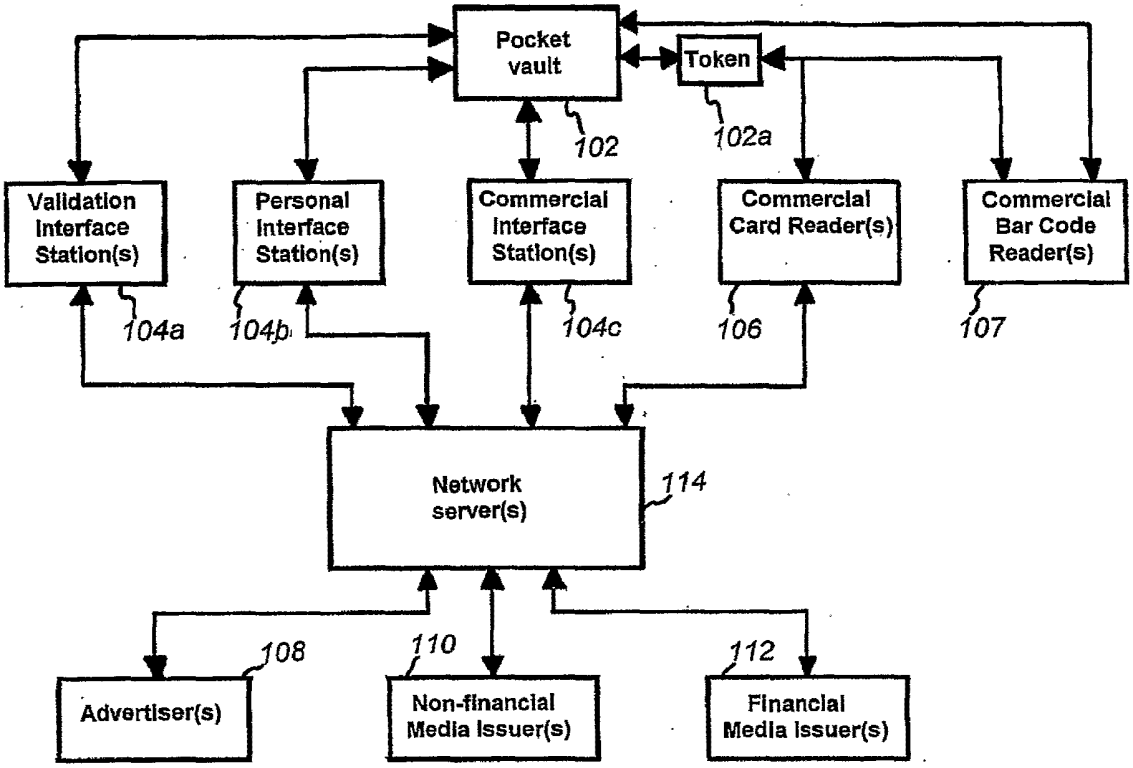

Pocket vault
Token
102
102a
Validation Interface Station(s)
Personal Interface Station(s)
Commercial Interface Station(s)
Commercial Card Reader(s)
Commercial Bar Code Reader(s)
104a
104b
104c
106
107
Network server(s)
114
Advertiser(s)
Non-financial Media Issuer(s)
Financial Media Issuer(s)
108
110
112

Fig. 1

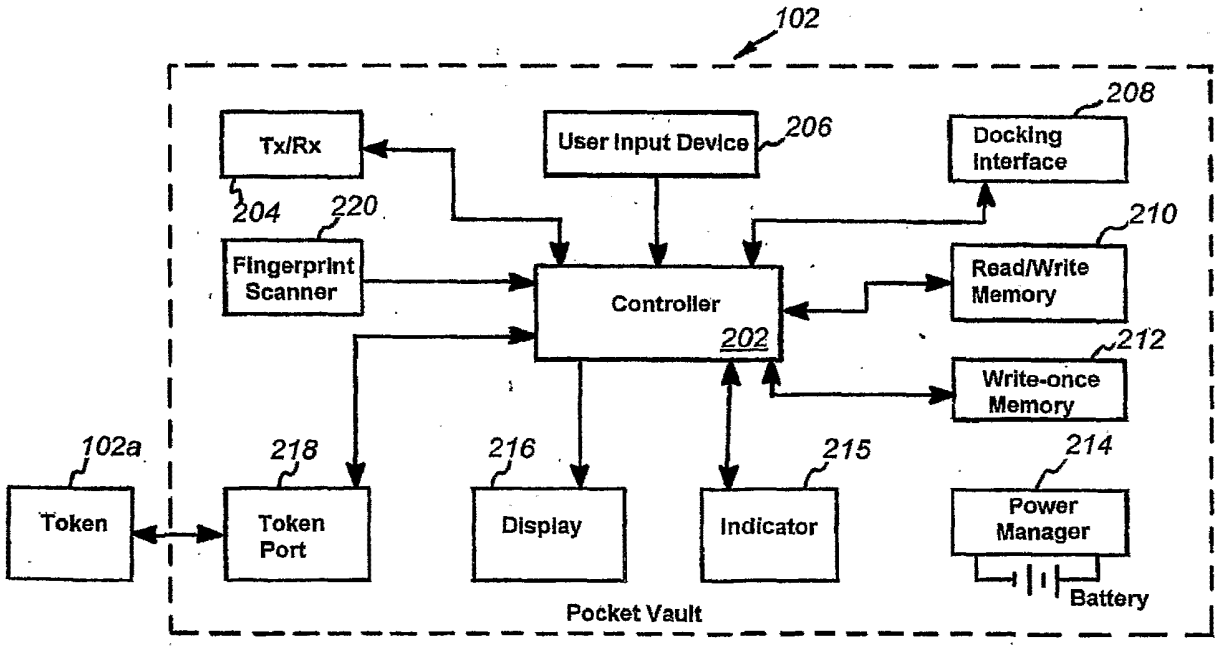

102
Tx/Rx
204
User Input Device
206
Docking Interface
208
Fingerprint Scanner
220
Controller
202
Read/Write Memory
210
Write-once Memory
212
Token
102a
Token Port
218
Display
216
Indicator
215
Power Manager
214
Battery
Pocket Vault

Fig. 2

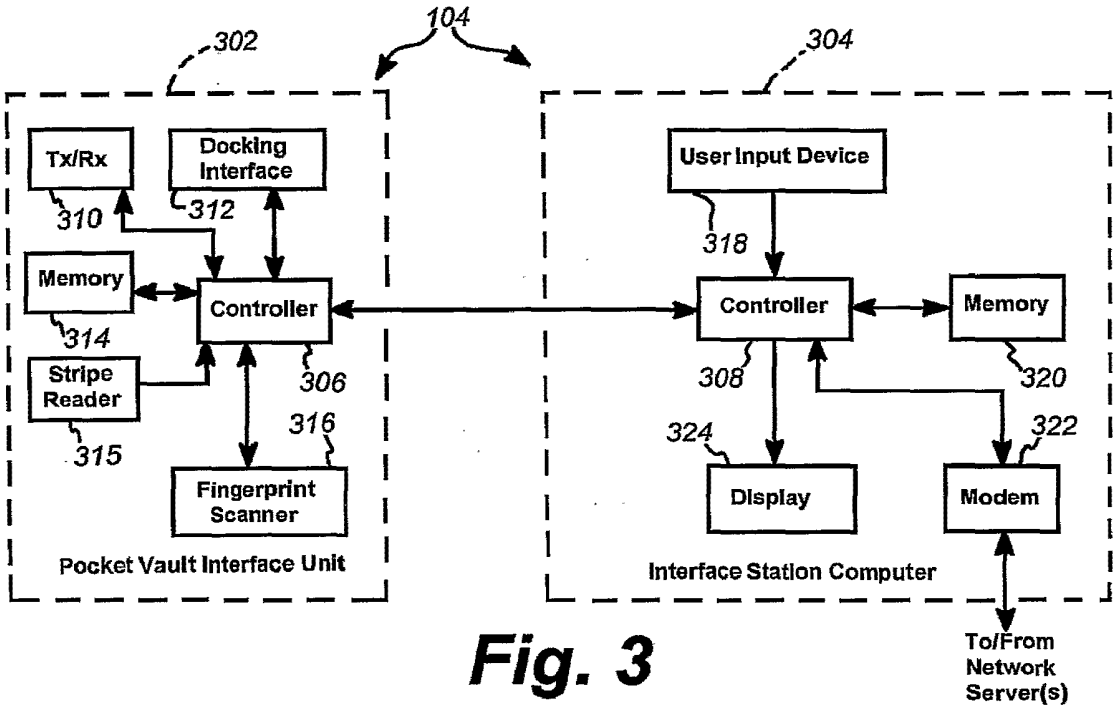

104
302
304
Tx/Rx
Docking Interface
310
312
Memory
Controller
314
306
Stripe Reader
315
316
Fingerprint Scanner
Pocket Vault Interface Unit
User Input Device
318
Controller
Memory
308
320
324
322
Display
Modem
Interface Station Computer
To/From Network Server(s)

Fig. 3

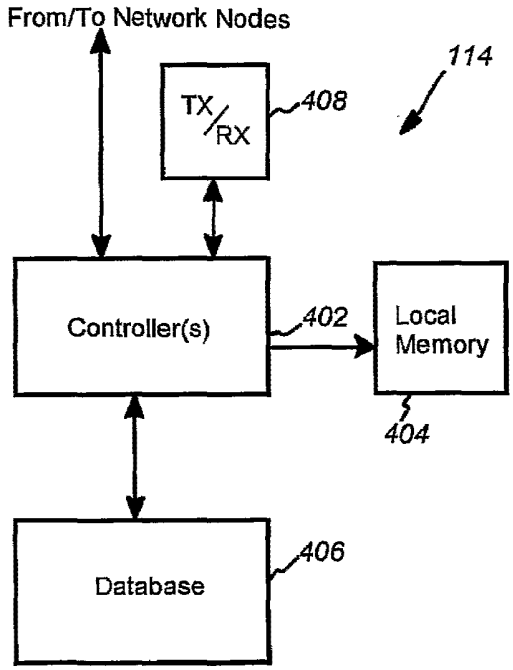

From/To Network Nodes
114
TX/RX
408
Controller(s)
402
Local Memory
404
Database
406

Fig. 4

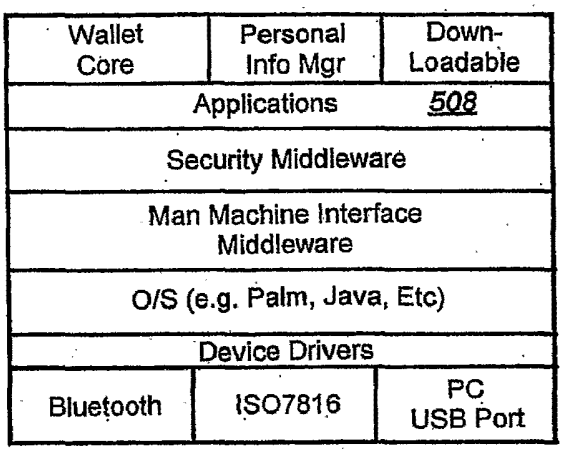

Wallet Core
Personal Info Mgr
Down-Loadable
Applications 508
Security Middleware
Man Machine Interface Middleware
O/S (e.g. Palm, Java, Etc)
Device Drivers
Bluetooth
ISO7816
PC USB Port

Fig. 5

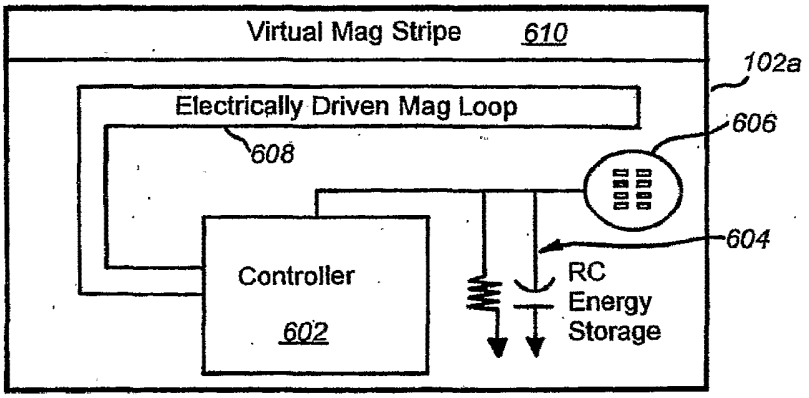

Virtual Mag Stripe 610
102a
Electrically Driven Mag Loop
608
606
604
Controller
602
RC
Energy
Storage

Fig. 6

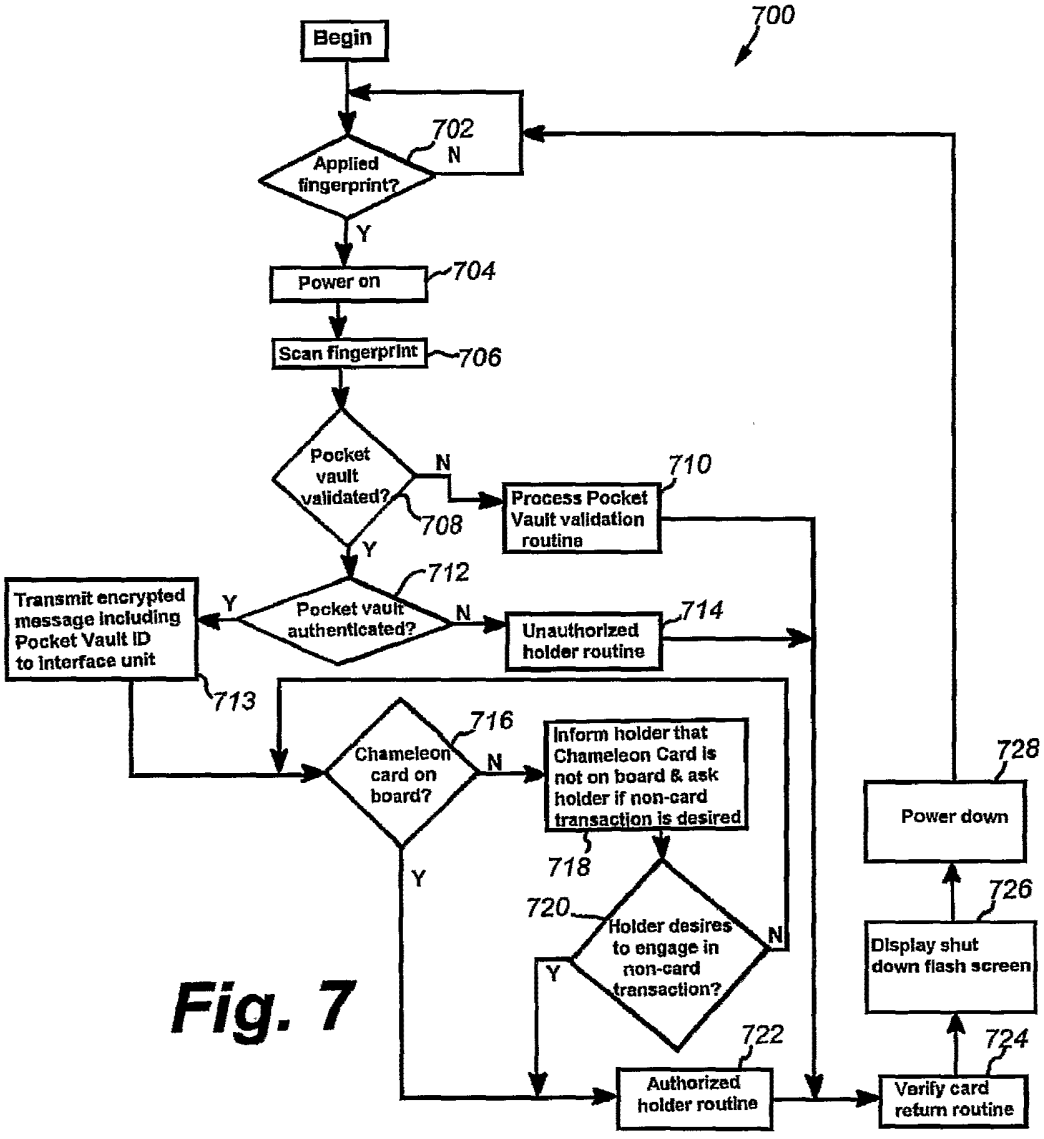

700
Begin
Applied fingerprint?
702
N
Y
Power on
704
Scan fingerprint
706
Pocket vault validated?
N
708
710
Process Pocket Vault validation routine
Y
Pocket vault authenticated?
712
Y
N
Transmit encrypted message including Pocket Vault ID to interface unit
713
Unauthorized holder routine
714
Chameleon card on board?
716
N
Y
Inform holder that Chameleon Card is not on board & ask holder if non-card transaction is desired
718
720
Holder desires to engage in non-card transaction?
Y
N
Authorized holder routine
722
Verify card return routine
724
Display shut down flash screen
726
Power down
728

Fig. 7

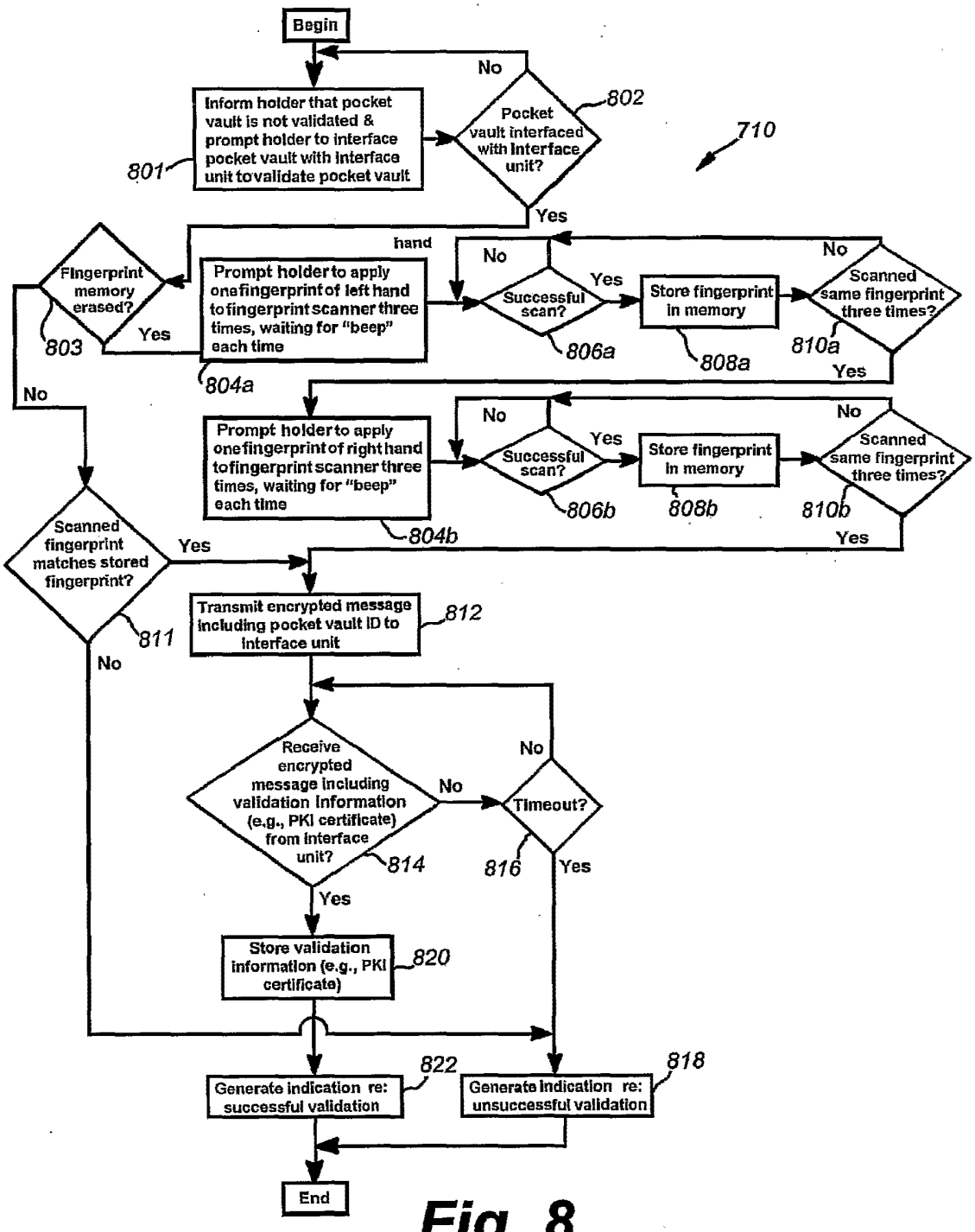

Begin
Inform holder that pocket vault is not validated & prompt holder to interface pocket vault with interface unit to validate pocket vault
801
Pocket vault interfaced with interface unit?
802
No
Yes
710
Fingerprint memory erased?
803
Yes
Prompt holder to apply one fingerprint of left hand to fingerprint scanner three times, waiting for "beep" each time
804a
Successful scan?
806a
No
Yes
Store fingerprint in memory
808a
Scanned same fingerprint three times?
810a
No
Yes
No
Prompt holder to apply one fingerprint of right hand to fingerprint scanner three times, waiting for "beep" each time
804b
Successful scan?
806b
No
Yes
Store fingerprint in memory
808b
Scanned same fingerprint three times?
810b
No
Yes
Scanned fingerprint matches stored fingerprint?
811
Yes
No
Transmit encrypted message including pocket vault ID to interface unit
812
Receive encrypted message including validation information (e.g., PKI certificate) from interface unit?
814
No
Yes
Timeout?
816
No
Yes
Store validation information (e.g., PKI certificate)
820
Generate indication re: successful validation
822
Generate indication re: unsuccessful validation
818
End

Fig. 8

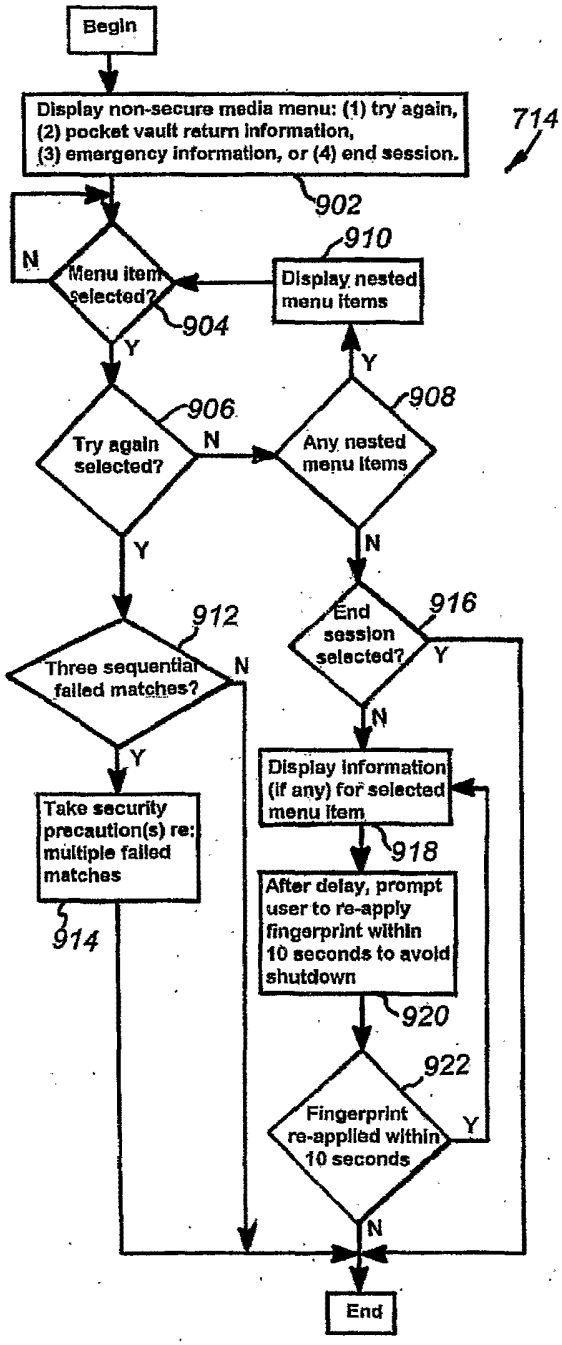

Begin
Display non-secure media menu: (1) try again, (2) pocket vault return information, (3) emergency information, or (4) end session.
714
902
910
Menu item selected?
904
Display nested menu items
N
Y
906
Try again selected?
908
Any nested menu items
912
Three sequential failed matches?
916
End session selected?
Take security precaution(s) re: multiple failed matches
914
Display information (if any) for selected menu item
918
After delay, prompt user to re-apply fingerprint within 10 seconds to avoid shutdown
920
922
Fingerprint re-applied within 10 seconds
End

Fig. 9

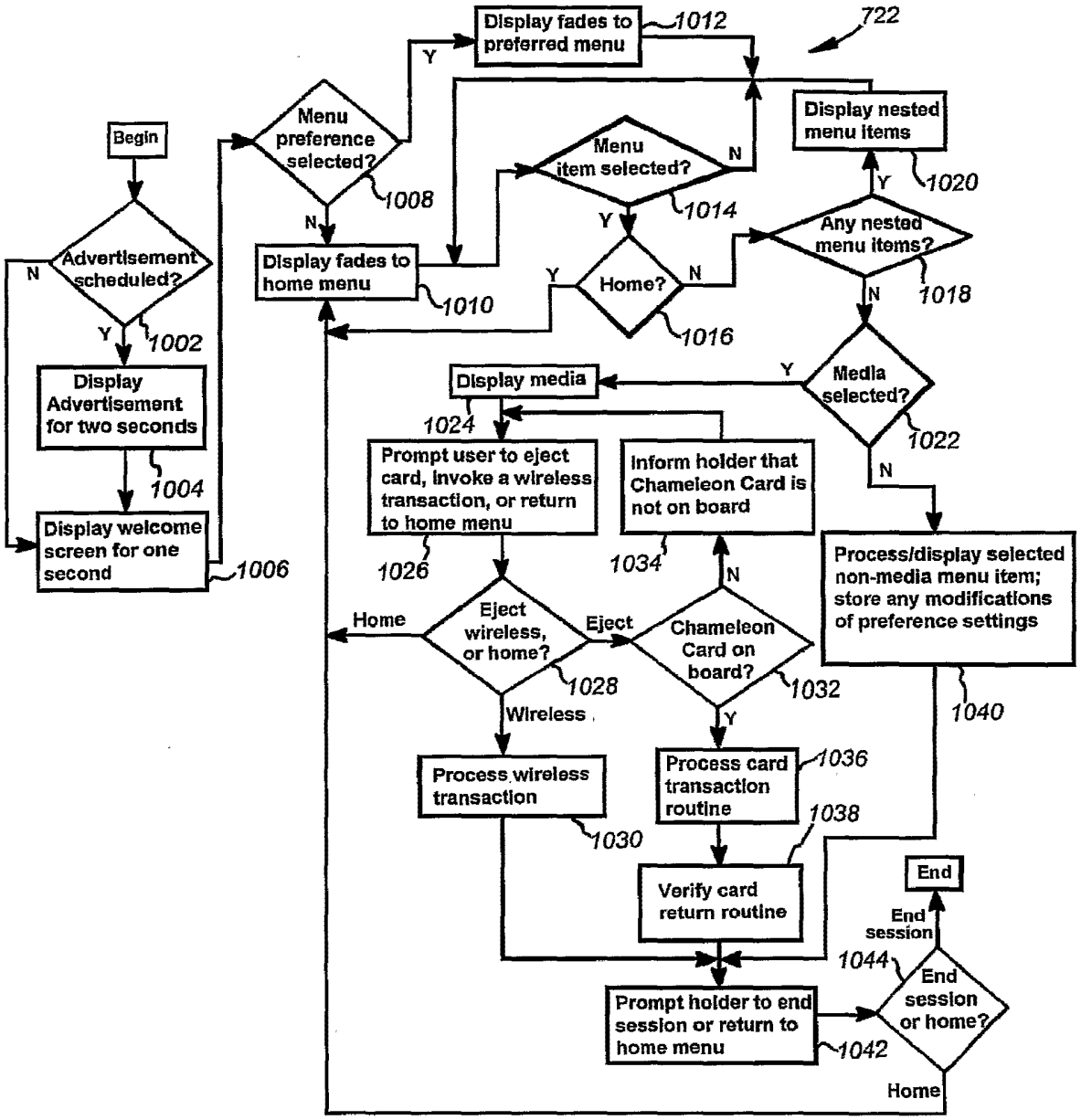

Begin
Advertisement scheduled?
1002
Display Advertisement for two seconds
1004
Display welcome screen for one second
1006
Menu preference selected?
1008
Display fades to home menu
1010
Display fades to preferred menu
1012
Menu item selected?
1014
Home?
1016
Any nested menu items?
1018
Display nested menu items
1020
Media selected?
1022
Display media
1024
Prompt user to eject card, invoke a wireless transaction, or return to home menu
1026
Eject wireless, or home?
1028
Process wireless transaction
1030
Chameleon Card on board?
1032
Inform holder that Chameleon Card is not on board
1034
Process card transaction routine
1036
Verify card return routine
1038
Process/display selected non-media menu item; store any modifications of preference settings
1040
Prompt holder to end session or return to home menu
1042
End session or home?
1044
End session
End
Home
Eject
Wireless
Y
N
722

Fig. 10

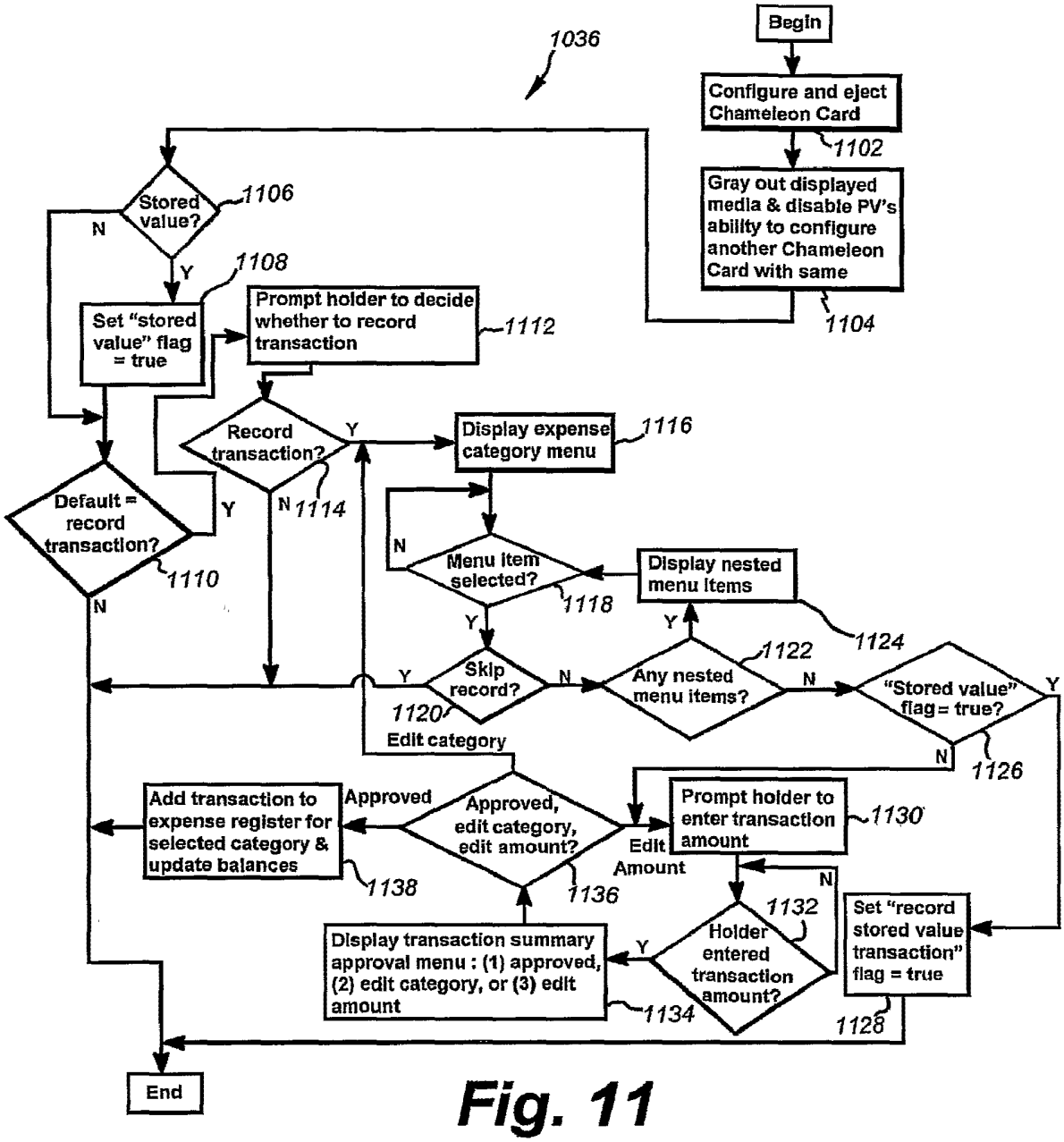

1036
Begin
Configure and eject Chameleon Card
1102
Gray out displayed media & disable PV's ability to configure another Chameleon Card with same
1104
Stored value?
1106
N
Y
1108
Set "stored value" flag = true
Prompt holder to decide whether to record transaction
1112
Record transaction?
Y
N
1114
Display expense category menu
1116
Default = record transaction?
Y
N
1110
N
Menu item selected?
1118
Display nested menu items
1124
Y
Y
Skip record?
Y
N
1120
Edit category
Any nested menu items?
1122
N
"Stored value" flag = true?
Y
N
1126
Add transaction to expense register for selected category & update balances
1138
Approved
Approved, edit category, edit amount?
1136
Edit Amount
Prompt holder to enter transaction amount
1130
N
1132
Holder entered transaction amount?
Y
Display transaction summary approval menu : (1) approved, (2) edit category, or (3) edit amount
1134
Set "record stored value transaction" flag = true
1128
End

Fig. 11

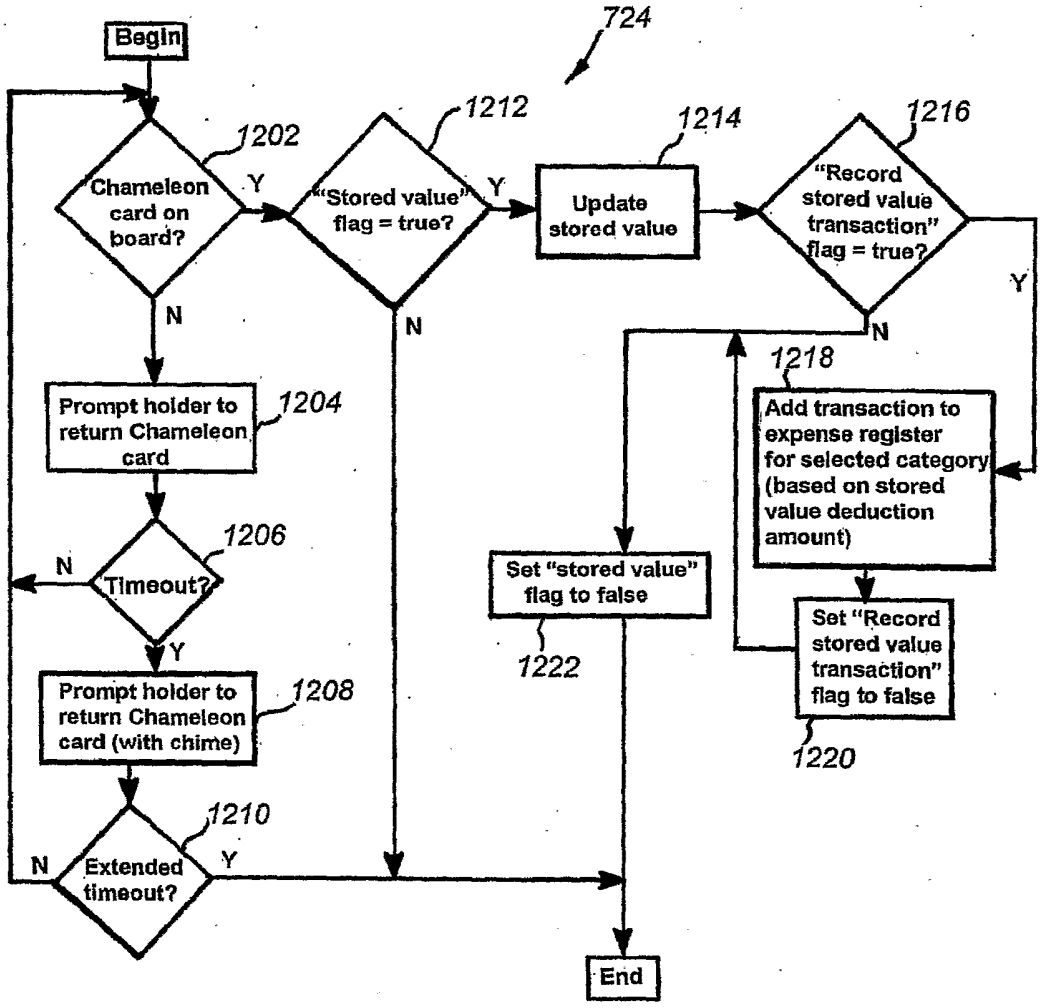

724
Begin
1202
Chameleon card on board?
Y
N
1212
"Stored value" flag = true?
Y
N
1214
Update stored value
1216
"Record stored value transaction" flag = true?
Y
N
1218
Add transaction to expense register for selected category (based on stored value deduction amount)
Set "Record stored value transaction" flag to false
1220
Set "stored value" flag to false
1222
Prompt holder to return Chameleon card
1204
1206
Timeout?
N
Y
Prompt holder to return Chameleon card (with chime)
1208
1210
Extended timeout?
N
Y
End

Fig. 12

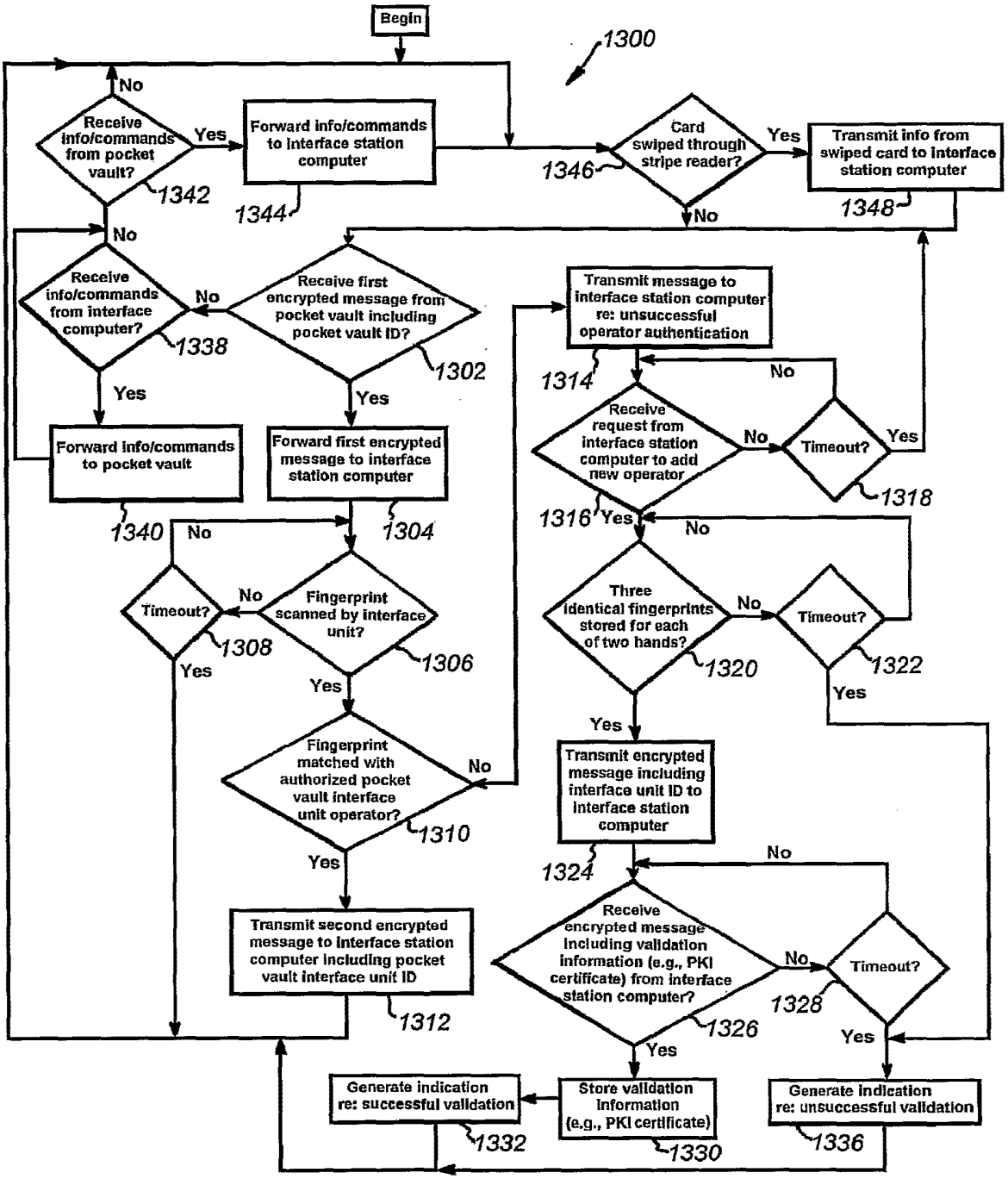

Begin
1300
Receive info/commands from pocket vault?
1342
Yes
No
Forward info/commands to interface station computer
1344
Card swiped through stripe reader?
1346
Yes
No
Transmit info from swiped card to interface station computer
1348
Receive info/commands from interface computer?
1338
No
Yes
Receive first encrypted message from pocket vault including pocket vault ID?
1302
Yes
No
Forward info/commands to pocket vault
1340
Forward first encrypted message to interface station computer
1304
Timeout?
1308
No
Yes
Fingerprint scanned by interface unit?
1306
No
Yes
Fingerprint matched with authorized pocket vault interface unit operator?
1310
No
Yes
Transmit second encrypted message to interface station computer including pocket vault interface unit ID
1312
Transmit message to interface station computer re: unsuccessful operator authentication
1314
Receive request from interface station computer to add new operator
1316
No
Yes
Timeout?
1318
No
Yes
Three identical fingerprints stored for each of two hands?
1320
No
Yes
Timeout?
1322
No
Yes
Transmit encrypted message including interface unit ID to interface station computer
1324
Receive encrypted message including validation information (e.g., PKI certificate) from interface station computer?
1326
No
Yes
Timeout?
1328
No
Yes
Store validation information (e.g., PKI certificate)
1330
Generate indication re: successful validation
1332
Generate indication re: unsuccessful validation
1336

Fig. 13

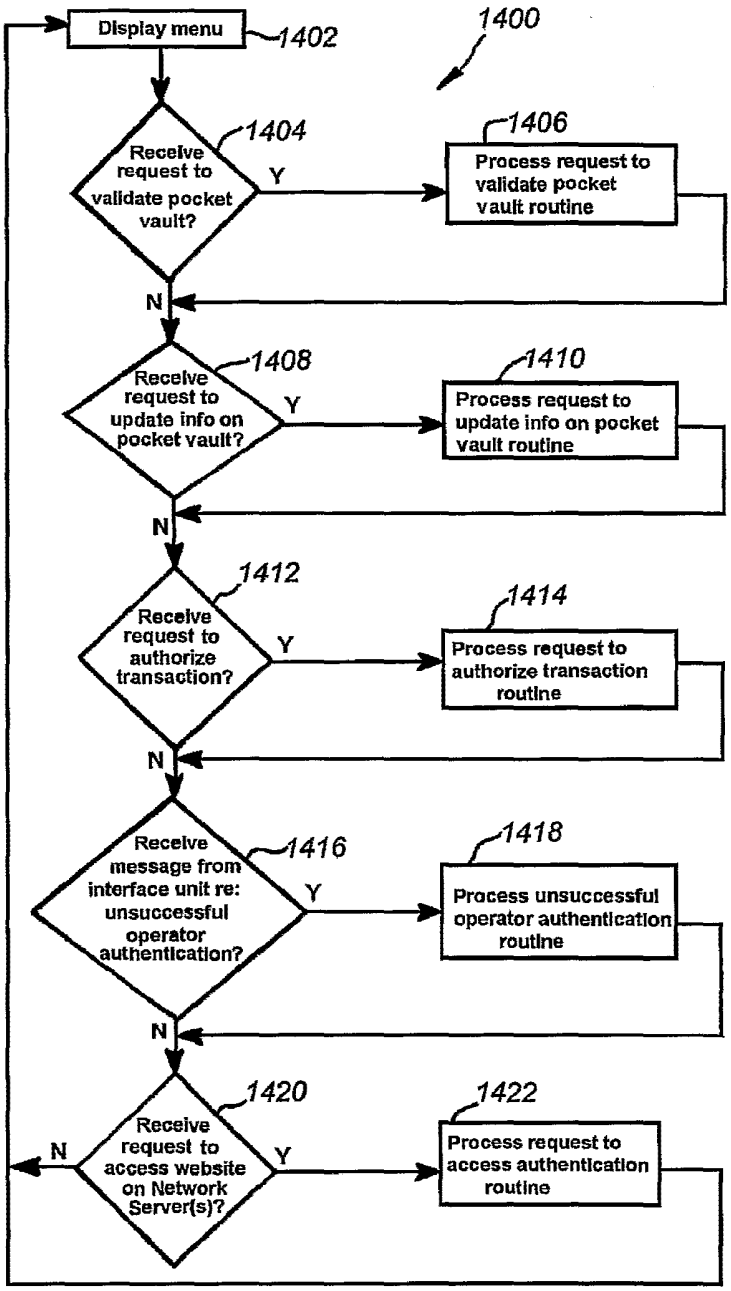

Display menu
1402
1400
Receive request to validate pocket vault?
1404
Y
1406
Process request to validate pocket vault routine
N
Receive request to update info on pocket vault?
1408
Y
1410
Process request to update info on pocket vault routine
N
Receive request to authorize transaction?
1412
Y
1414
Process request to authorize transaction routine
N
Receive message from interface unit re: unsuccessful operator authentication?
1416
Y
1418
Process unsuccessful operator authentication routine
N
Receive request to access website on Network Server(s)?
1420
N
Y
1422
Process request to access authentication routine

Fig. 14

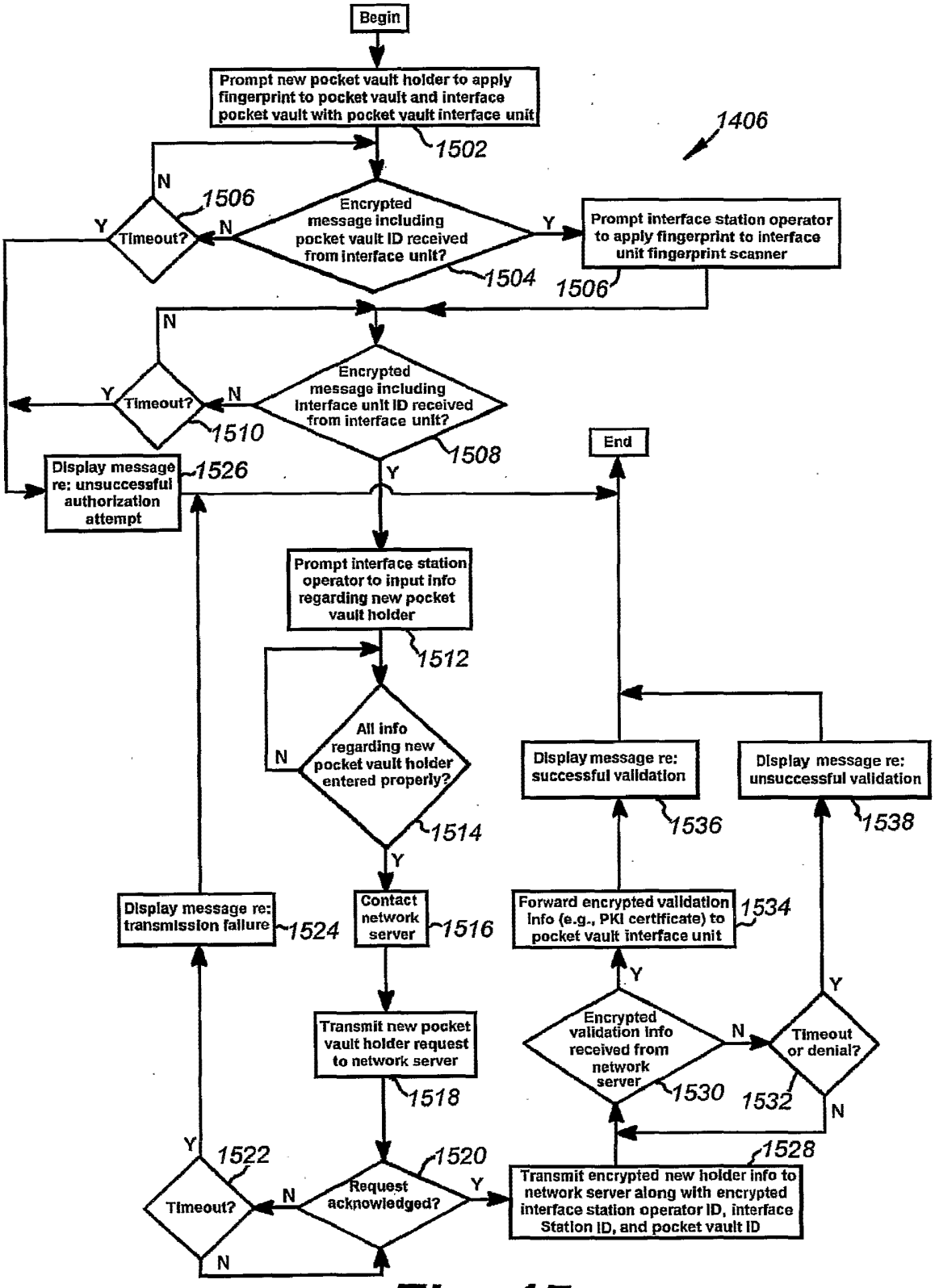

Begin
Prompt new pocket vault holder to apply fingerprint to pocket vault and interface pocket vault with pocket vault interface unit
1502
1406
Encrypted message including pocket vault ID received from interface unit?
1504
Timeout?
1506
Prompt interface station operator to apply fingerprint to interface unit fingerprint scanner
1506
Encrypted message including interface unit ID received from interface unit?
1508
Timeout?
1510
End
Display message re: unsuccessful authorization attempt
1526
Prompt interface station operator to input info regarding new pocket vault holder
1512
All info regarding new pocket vault holder entered properly?
1514
Display message re: successful validation
1536
Display message re: unsuccessful validation
1538
Display message re: transmission failure
1524
Contact network server
1516
Forward encrypted validation info (e.g., PKI certificate) to pocket vault interface unit
1534
Transmit new pocket vault holder request to network server
1518
Encrypted validation info received from network server
1530
Timeout or denial?
1532
Request acknowledged?
1520
Timeout?
1522
Transmit encrypted new holder info to network server along with encrypted interface station operator ID, interface Station ID, and pocket vault ID
1528
Y
N

Fig. 15

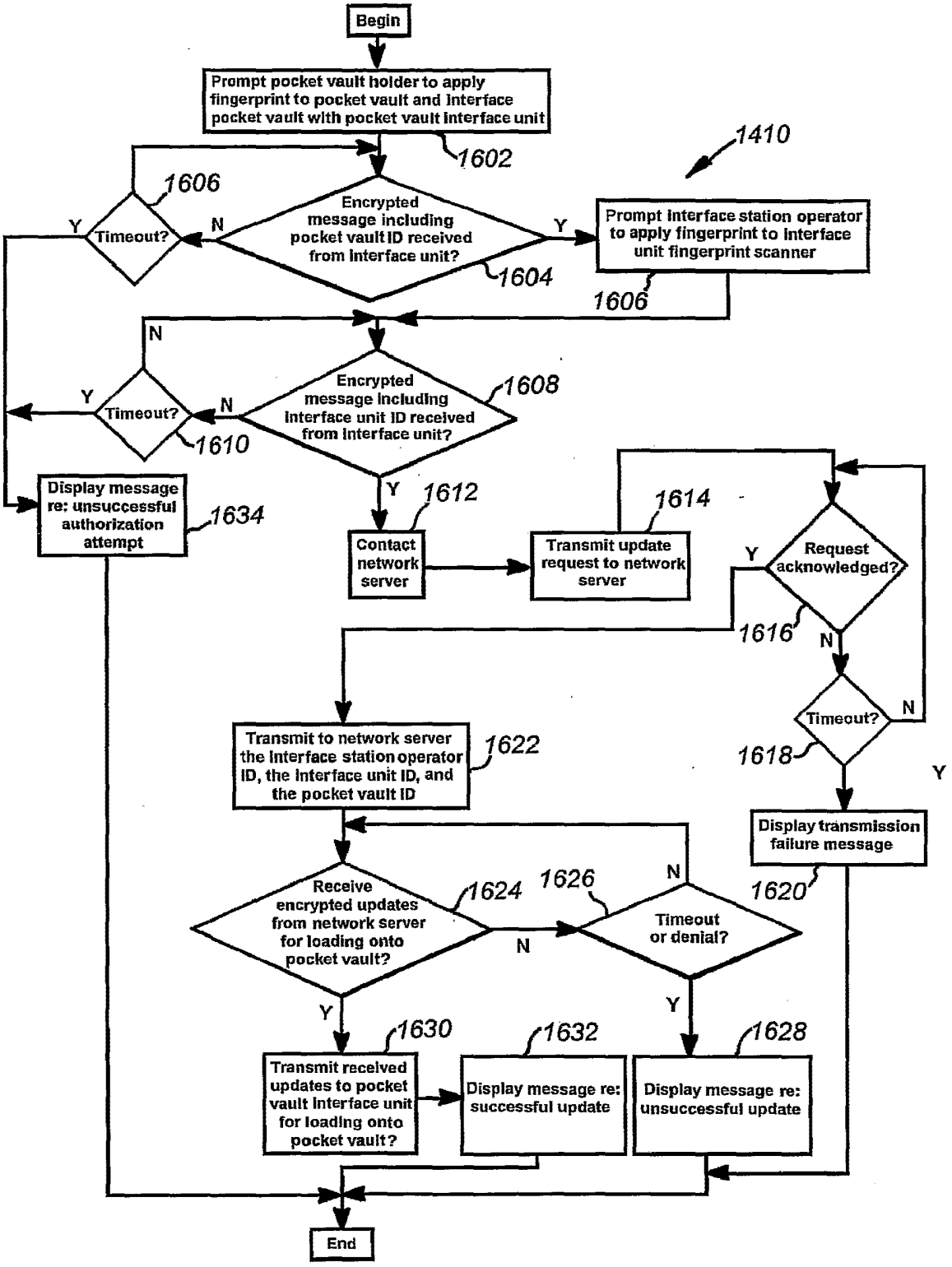

Begin
Prompt pocket vault holder to apply fingerprint to pocket vault and interface pocket vault with pocket vault interface unit
1602
1410
1606
Encrypted message including pocket vault ID received from interface unit?
1604
Timeout?
Y
N
Prompt interface station operator to apply fingerprint to interface unit fingerprint scanner
1606
N
Encrypted message including interface unit ID received from interface unit?
1608
Timeout?
1610
Y
N
Display message re: unsuccessful authorization attempt
1634
Y
1612
Contact network server
Transmit update request to network server
1614
Request acknowledged?
Y
1616
N
Timeout?
1618
N
Y
Transmit to network server the interface station operator ID, the interface unit ID, and the pocket vault ID
1622
Display transmission failure message
1620
Receive encrypted updates from network server for loading onto pocket vault?
1624
1626
Timeout or denial?
N
Y
Y
1630
1632
1628
Transmit received updates to pocket vault interface unit for loading onto pocket vault?
Display message re: successful update
Display message re: unsuccessful update
End

Fig. 16

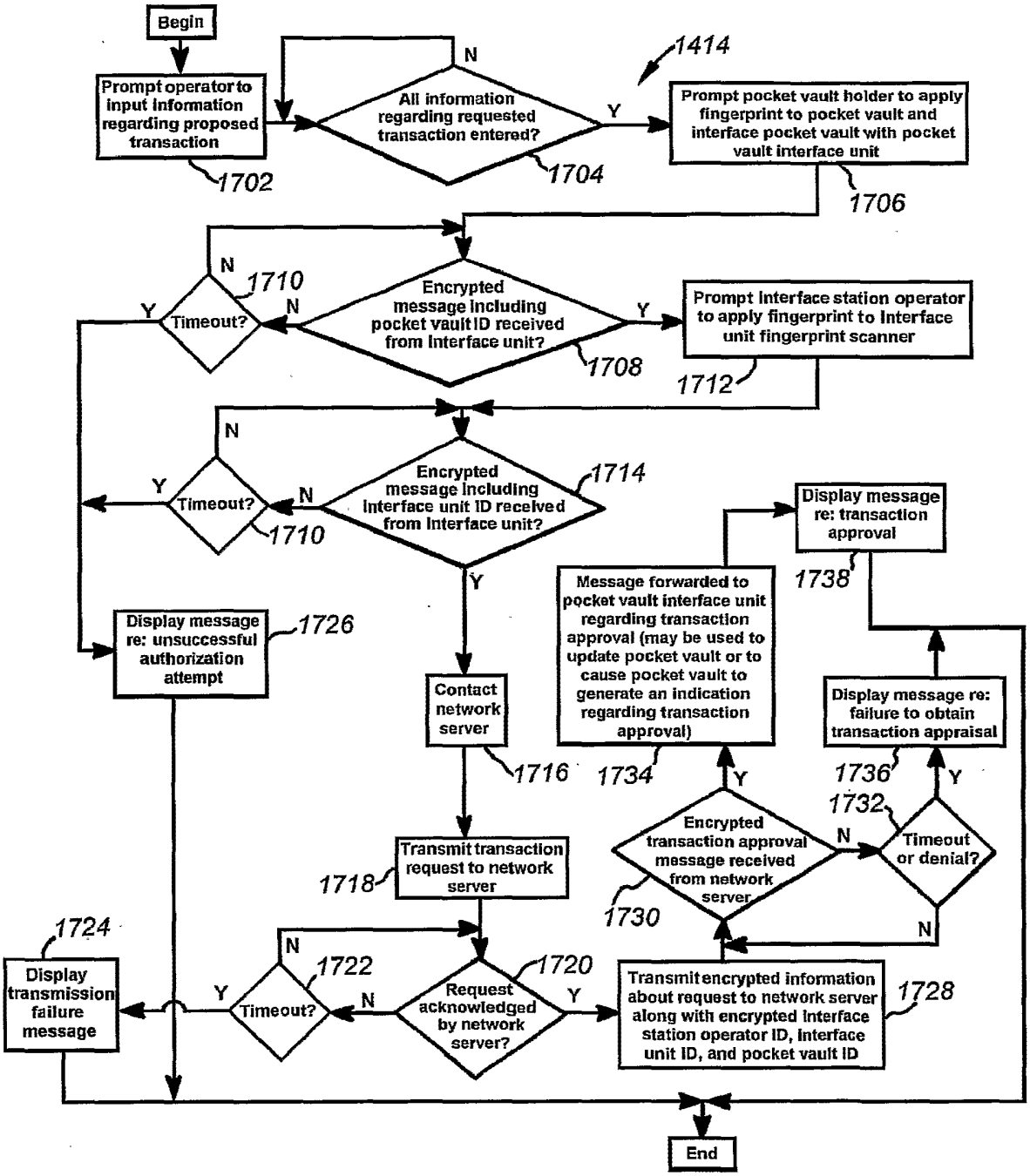

Begin
Prompt operator to input information regarding proposed transaction
1702
All information regarding requested transaction entered?
1704
N
Y
1414
Prompt pocket vault holder to apply fingerprint to pocket vault and interface pocket vault with pocket vault interface unit
1706
Encrypted message including pocket vault ID received from interface unit?
1708
Timeout?
1710
Prompt interface station operator to apply fingerprint to interface unit fingerprint scanner
1712
Encrypted message including interface unit ID received from interface unit?
1714
Timeout?
1710
Display message re: transaction approval
1738
Message forwarded to pocket vault interface unit regarding transaction approval (may be used to update pocket vault or to cause pocket vault to generate an indication regarding transaction approval)
1734
Display message re: failure to obtain transaction appraisal
1736
Display message re: unsuccessful authorization attempt
1726
Contact network server
1716
Encrypted transaction approval message received from network server
1730
Timeout or denial?
1732
Transmit transaction request to network server
1718
Display transmission failure message
1724
Timeout?
1722
Request acknowledged by network server?
1720
Transmit encrypted information about request to network server along with encrypted interface station operator ID, interface unit ID, and pocket vault ID
1728
End

Fig. 17

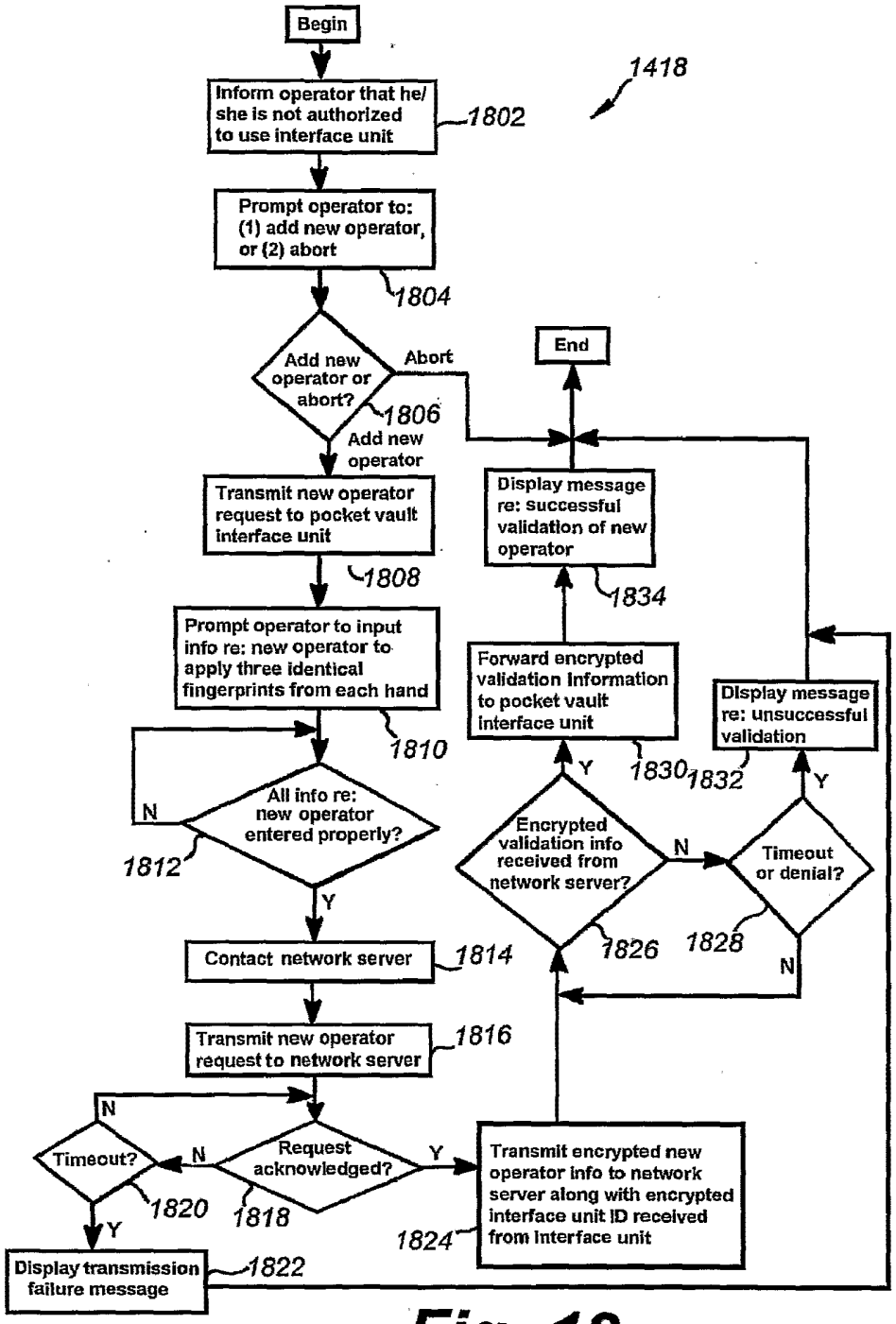

Begin
1418
Inform operator that he/she is not authorized to use interface unit
1802
Prompt operator to: (1) add new operator, or (2) abort
1804
Add new operator or abort?
1806
Abort
End
Add new operator
Transmit new operator request to pocket vault interface unit
1808
Display message re: successful validation of new operator
1834
Prompt operator to input info re: new operator to apply three identical fingerprints from each hand
1810
Forward encrypted validation information to pocket vault interface unit
1830
Display message re: unsuccessful validation
1832
N
All info re: new operator entered properly?
1812
Y
Y
Encrypted validation info received from network server?
1826
N
Timeout or denial?
1828
Y
N
Contact network server
1814
Transmit new operator request to network server
1816
N
Timeout?
1820
N
Request acknowledged?
1818
Y
Transmit encrypted new operator info to network server along with encrypted interface unit ID received from interface unit
1824
Y
Display transmission failure message
1822

Fig. 18

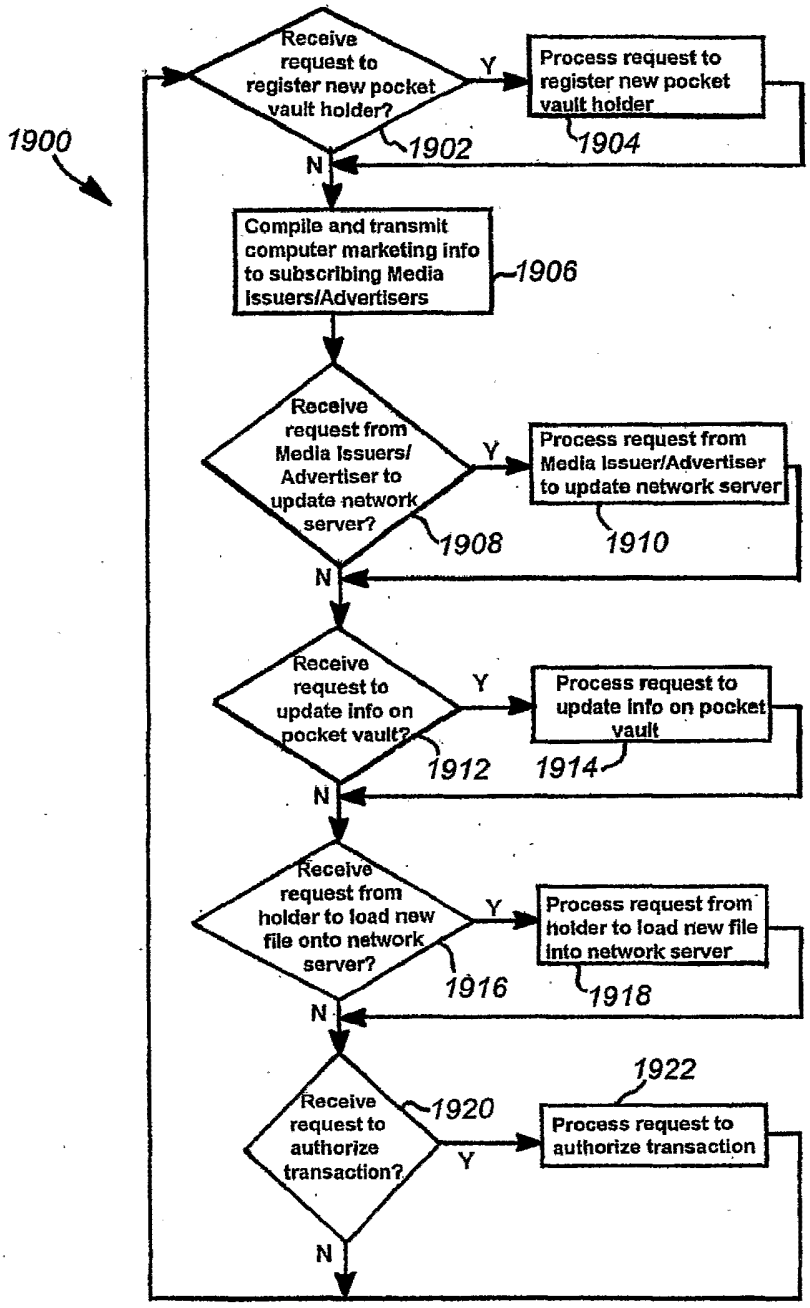

1900
Receive request to register new pocket vault holder?
1902
Y
Process request to register new pocket vault holder
1904
N
Compile and transmit computer marketing info to subscribing Media Issuers/Advertisers
1906
Receive request from Media Issuers/ Advertiser to update network server?
1908
Y
Process request from Media Issuer/Advertiser to update network server
1910
N
Receive request to update info on pocket vault?
1912
Y
Process request to update info on pocket vault
1914
N
Receive request from holder to load new file onto network server?
1916
Y
Process request from holder to load new file into network server
1918
N
Receive request to authorize transaction?
1920
Y
1922
Process request to authorize transaction
N

Fig. 19

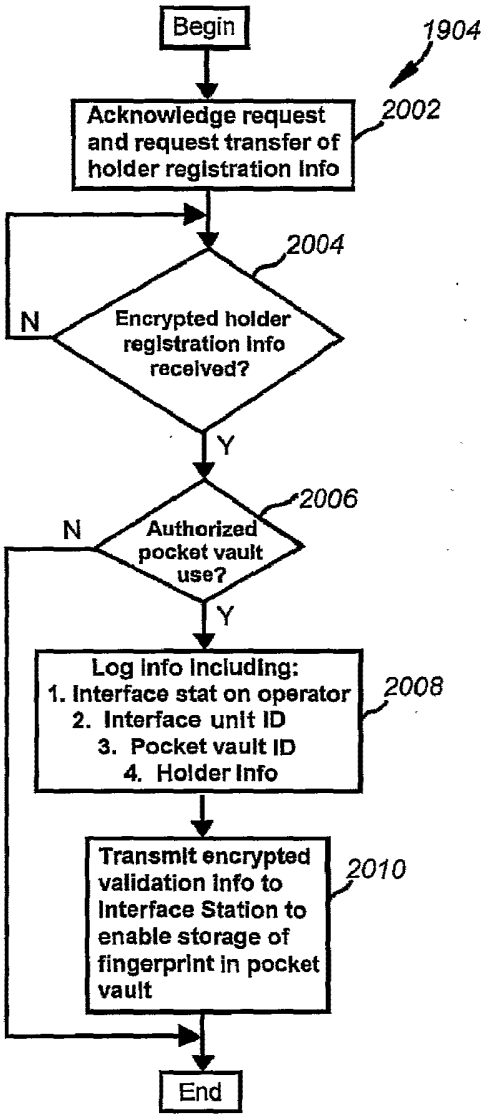

Begin
1904
Acknowledge request and request transfer of holder registration info
2002
2004
N
Encrypted holder registration info received?
Y
2006
N
Authorized pocket vault use?
Y
Log info including:
1. Interface stat on operator
2. Interface unit ID
3. Pocket vault ID
4. Holder info
2008
Transmit encrypted validation info to Interface Station to enable storage of fingerprint in pocket vault
2010
End

Fig. 20

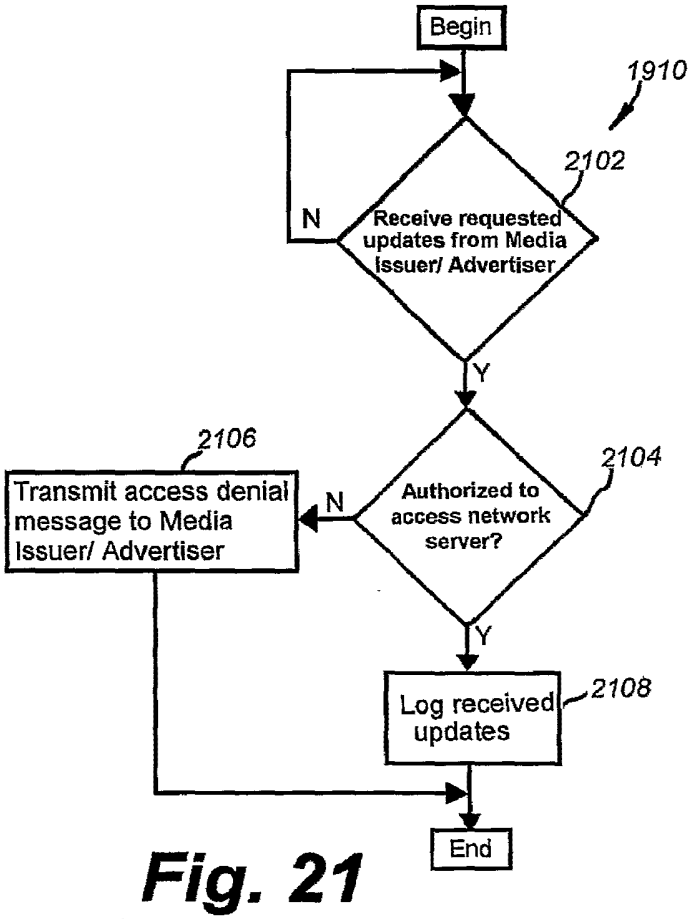

Begin
1910
2102
N
Receive requested updates from Media Issuer/ Advertiser
Y
2106
Transmit access denial message to Media Issuer/ Advertiser
N
2104
Authorized to access network server?
Y
Log received updates
2108
End

Fig. 21

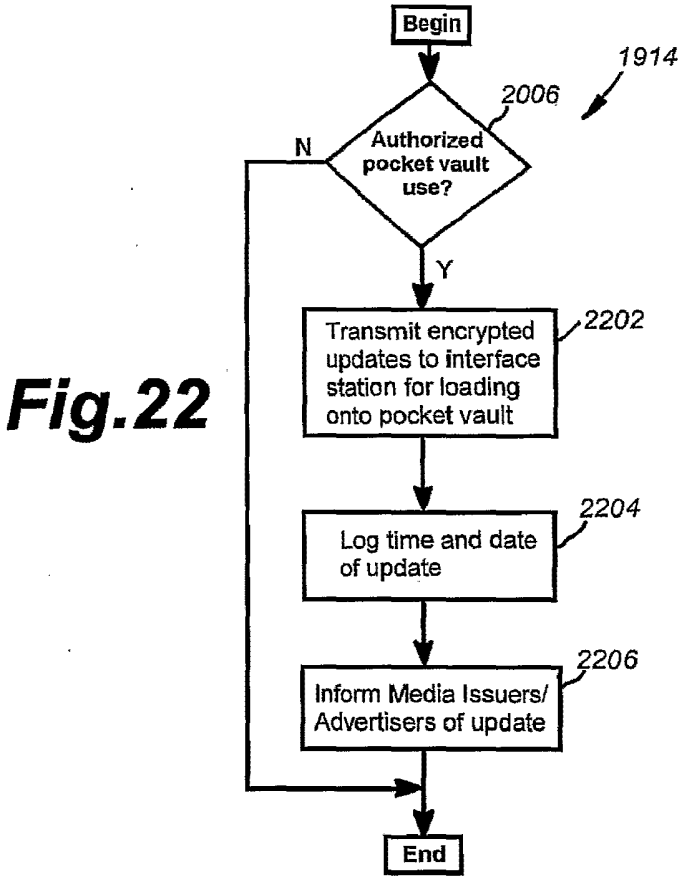

Begin
1914
2006
Authorized pocket vault use?
N
Y
Transmit encrypted updates to interface station for loading onto pocket vault
2202
Log time and date of update
2204
Inform Media Issuers/ Advertisers of update
2206
End

Fig.22

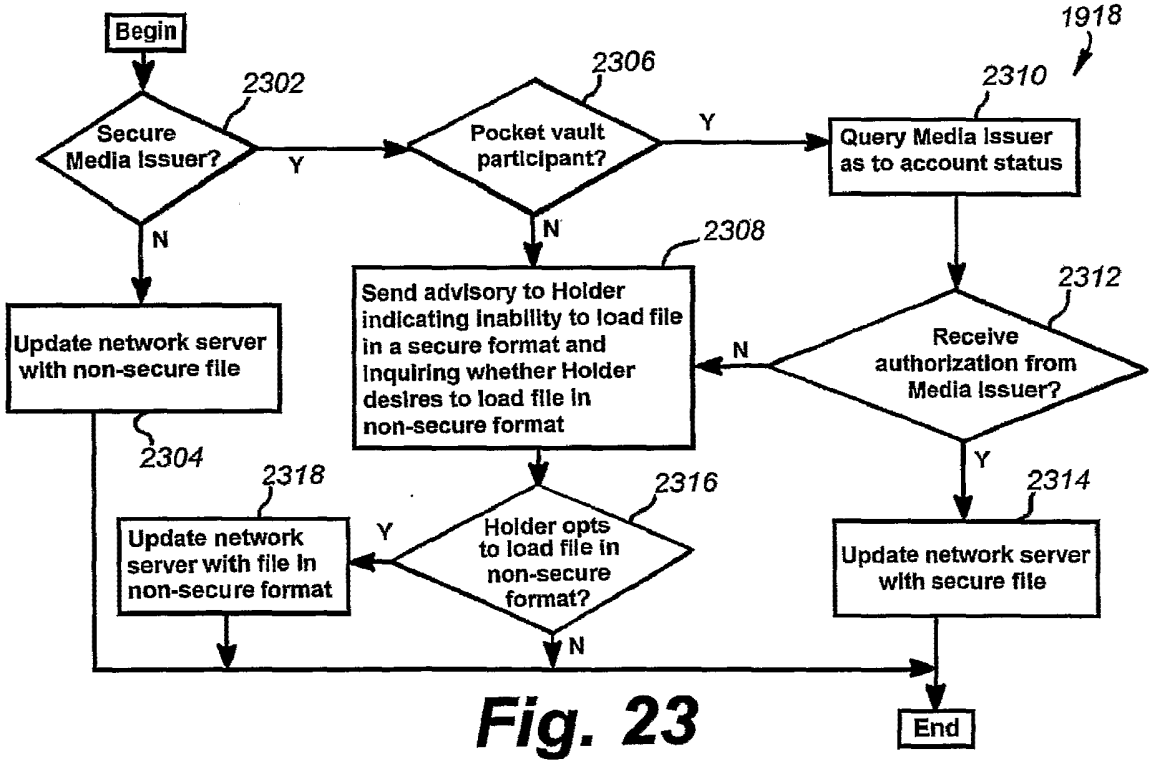

Begin
1918
2302
Secure Media Issuer?
Y
N
2306
Pocket vault participant?
Y
N
2310
Query Media Issuer as to account status
2308
Send advisory to Holder indicating inability to load file in a secure format and inquiring whether Holder desires to load file in non-secure format
2312
Receive authorization from Media Issuer?
N
Y
Update network server with non-secure file
2304
2318
Update network server with file in non-secure format
Y
2316
Holder opts to load file in non-secure format?
N
2314
Update network server with secure file
End

Fig. 23

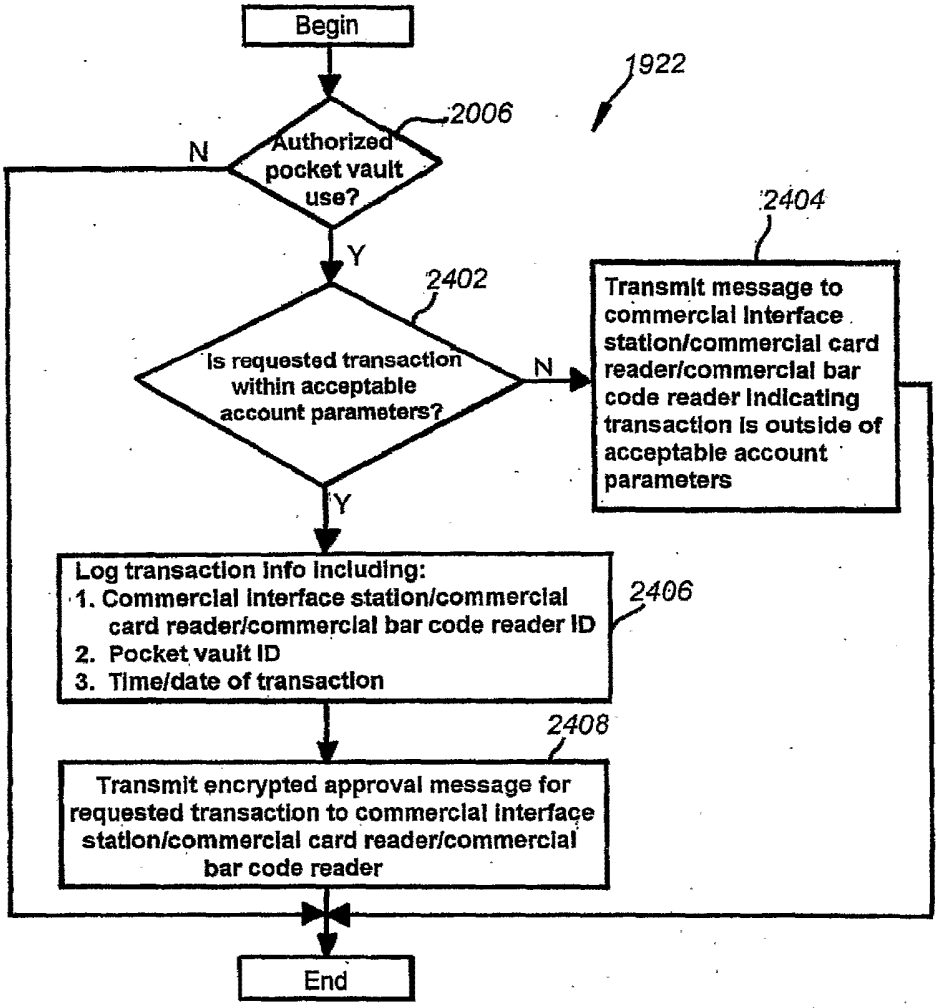

Begin
1922
2006
Authorized pocket vault use?
N
Y
2402
Is requested transaction within acceptable account parameters?
N
2404
Transmit message to commercial interface station/commercial card reader/commercial bar code reader indicating transaction is outside of acceptable account parameters
Y
Log transaction info including:
1. Commercial interface station/commercial card reader/commercial bar code reader ID
2. Pocket vault ID
3. Time/date of transaction
2406
2408
Transmit encrypted approval message for requested transaction to commercial interface station/commercial card reader/commercial bar code reader
End

Fig. 24

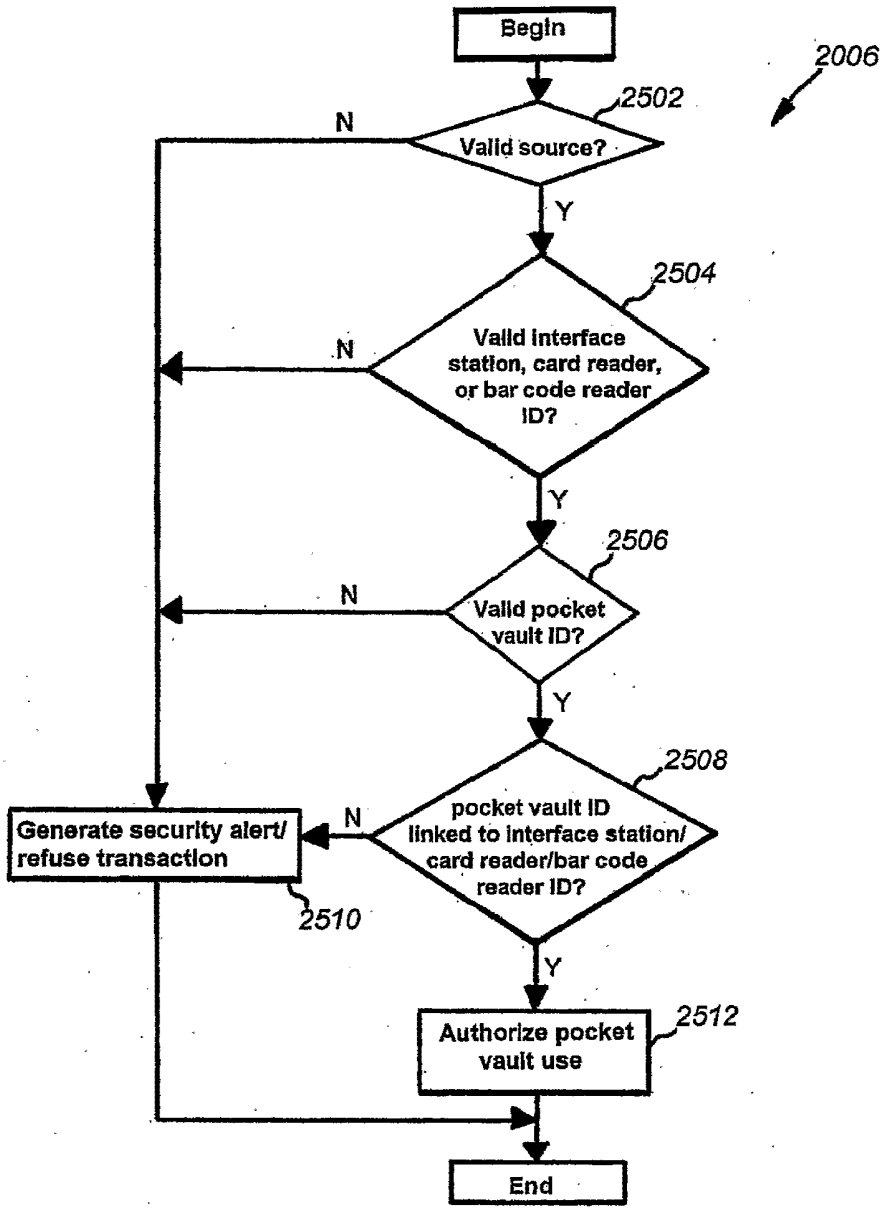

Begin
2006
2502
Valid source?
N
Y
2504
Valid interface station, card reader, or bar code reader ID?
N
Y
2506
Valid pocket vault ID?
N
Y
2508
pocket vault ID linked to interface station/ card reader/bar code reader ID?
N
Y
Generate security alert/ refuse transaction
2510
Authorize pocket vault use
2512
End

Fig. 25

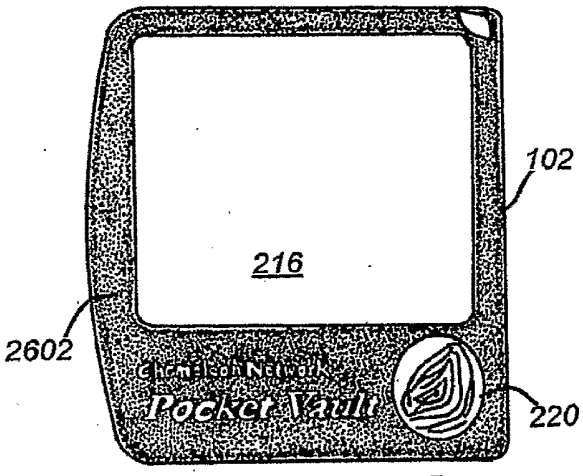


Fig. 26A

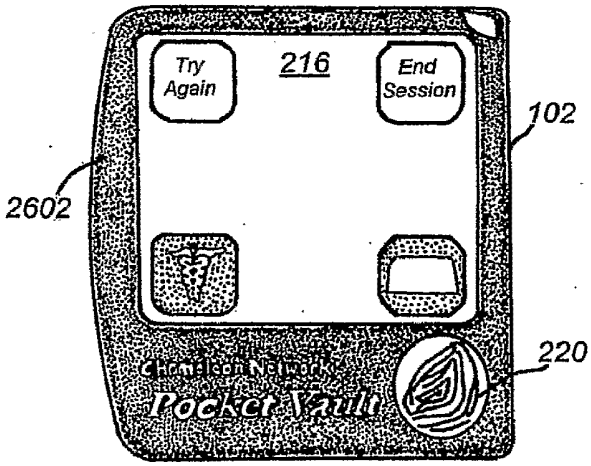


Fig. 26B

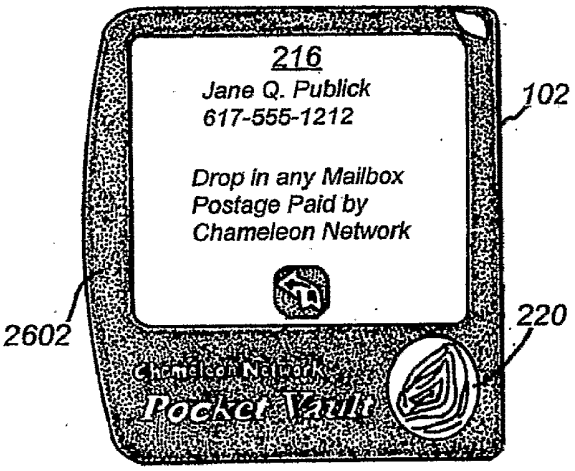


Fig. 26C

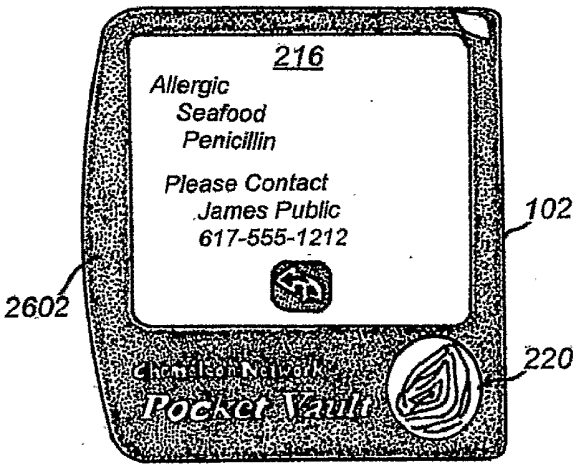


Fig. 26D

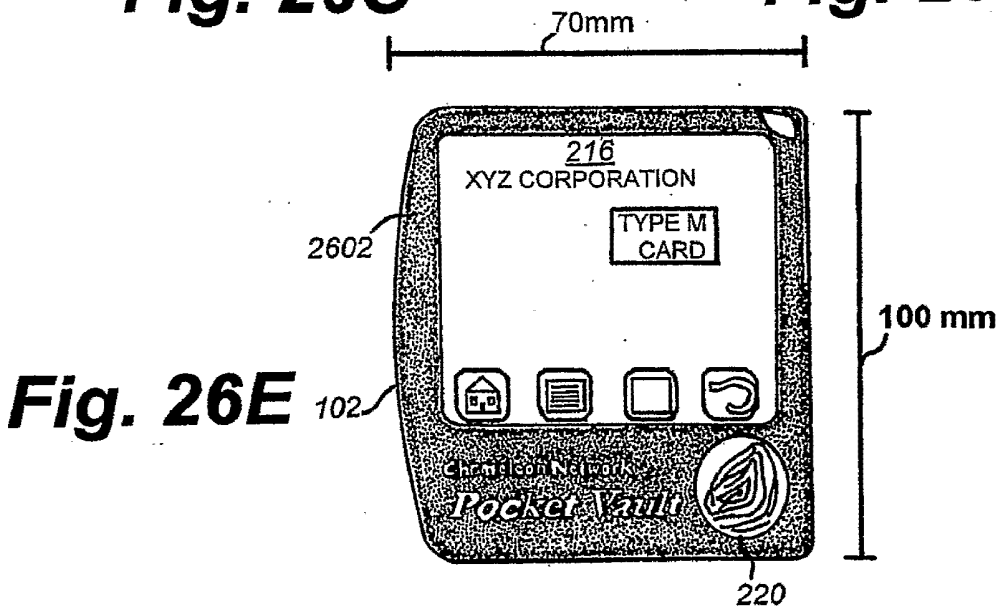


Fig. 26E

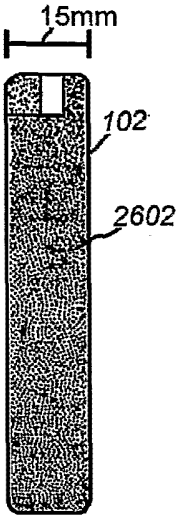


Fig. 26F

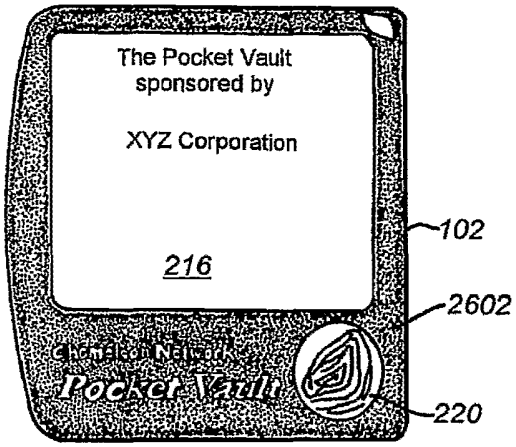


Fig. 26G

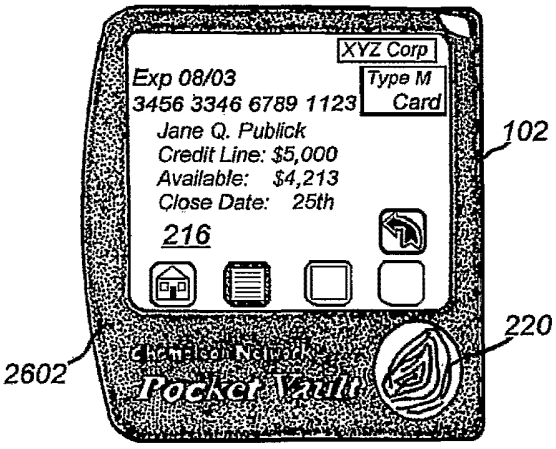


Fig. 26H

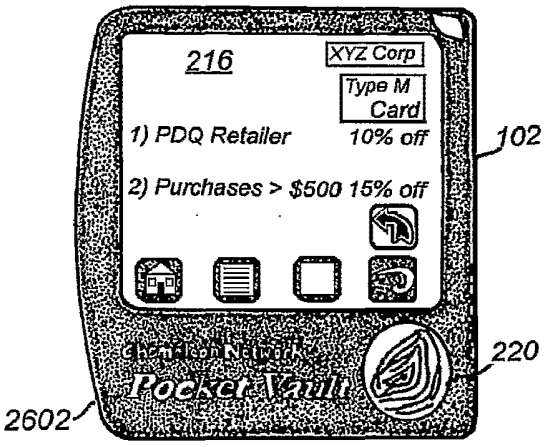


Fig. 26I

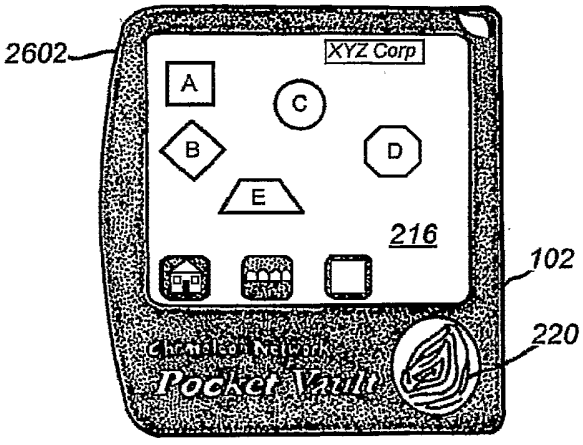


Fig. 26J

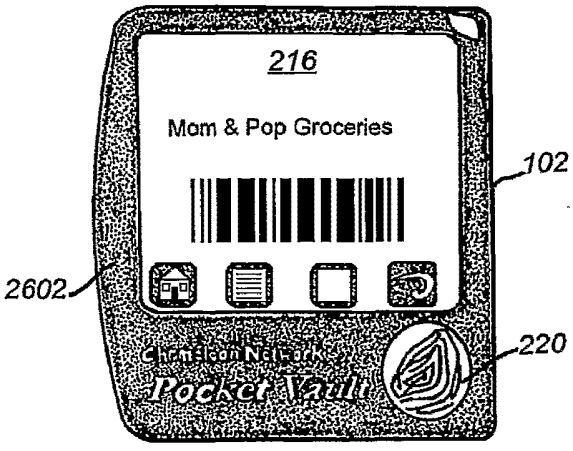


Fig. 26K

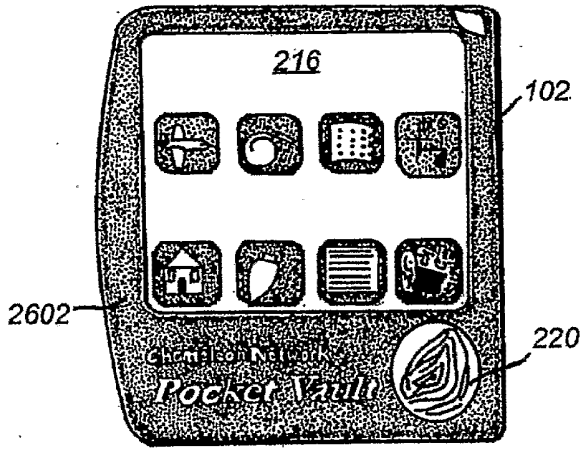


Fig. 26L

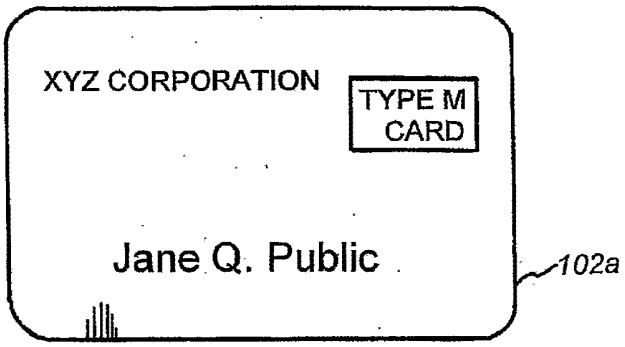


Fig. 26M

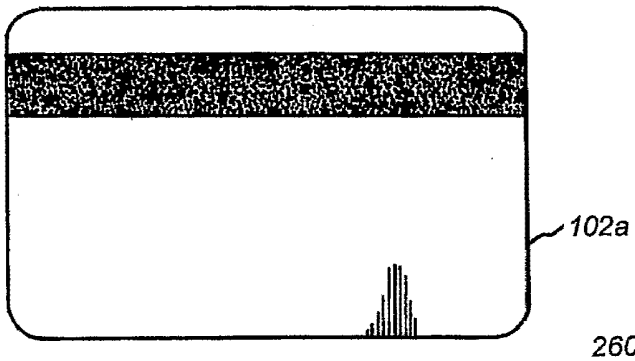


Fig. 26N

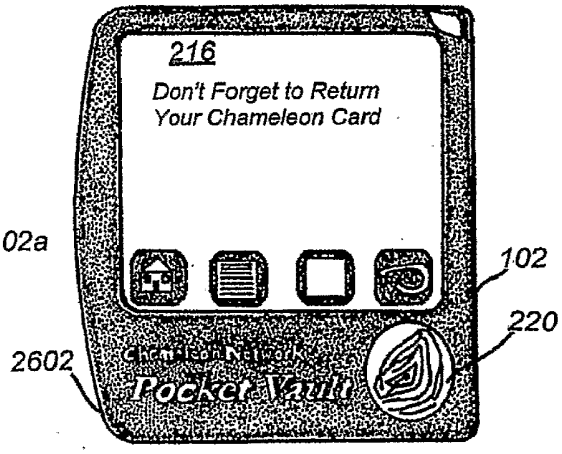


Fig. 26O

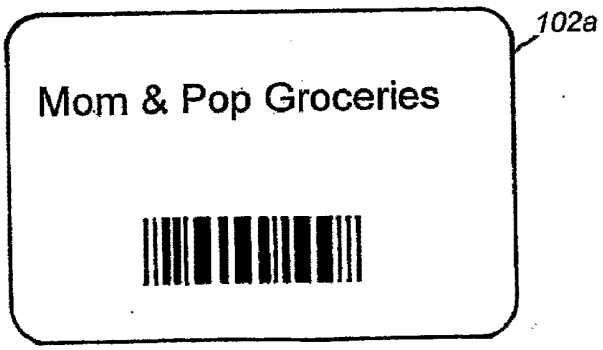


Fig. 26P

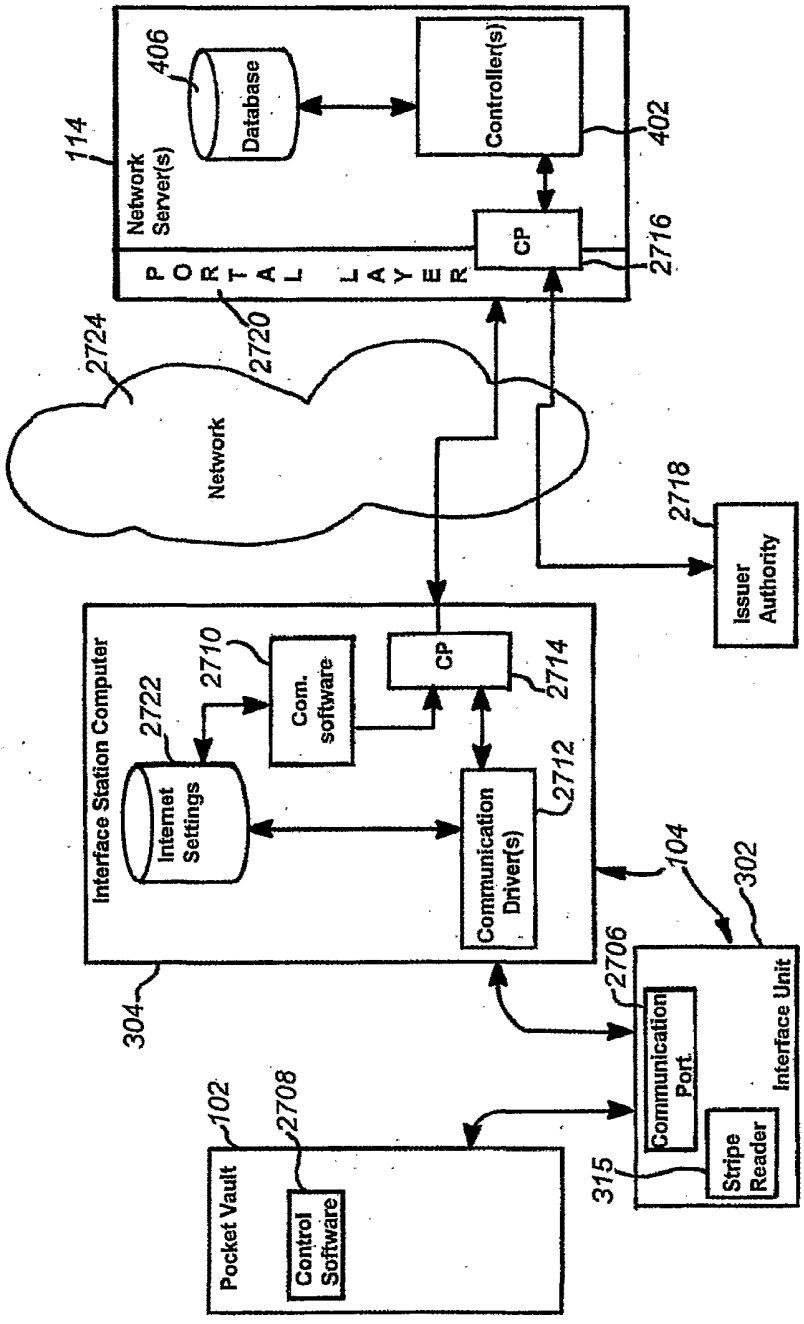

114
Network Server(s)
406
Database
Controller(s)
402
PORTAL LAYER
CP
2716
2720
2724
Network
2718
Issuer Authority
Interface Station Computer
2710
Com. software
CP
2714
2722
Internet Settings
2712
Communication Driver(s)
104
302
304
2706
Communication Port
Stripe Reader
315
Interface Unit
102
2708
Pocket Vault
Control Software

Fig. 27

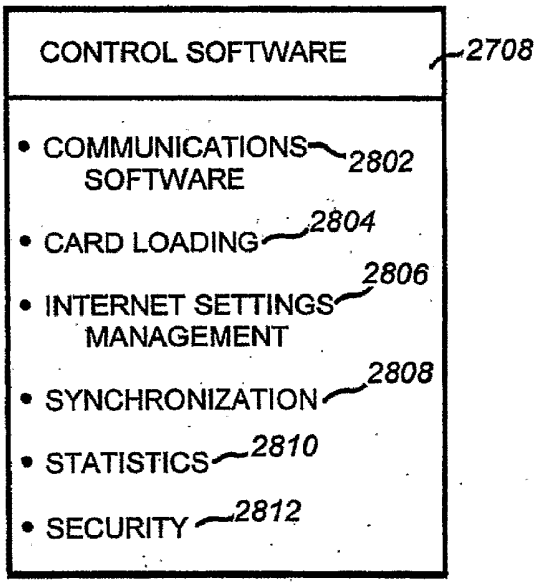

CONTROL SOFTWARE
2708
• COMMUNICATIONS SOFTWARE
2802
• CARD LOADING
2804
• INTERNET SETTINGS MANAGEMENT
2806
• SYNCHRONIZATION
2808
• STATISTICS
2810
• SECURITY
2812

Fig. 28

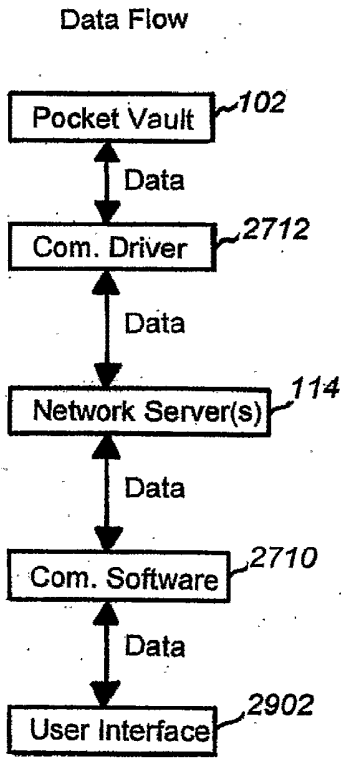

Data Flow
Pocket Vault
102
Data
Com. Driver
2712
Data
Network Server(s)
114
Data
Com. Software
2710
Data
User Interface
2902

Fig. 29

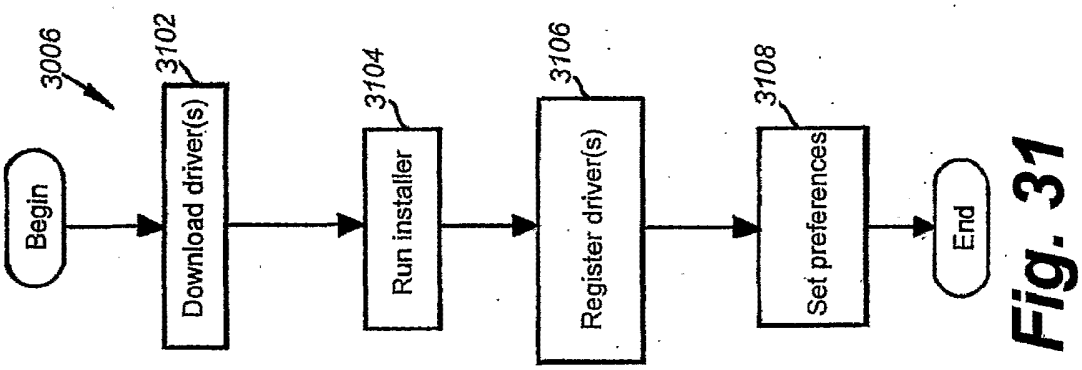

3006
3102
3104
3106
3108
Begin
Download driver(s)
Run installer
Register driver(s)
Set preferences
End

Fig. 31

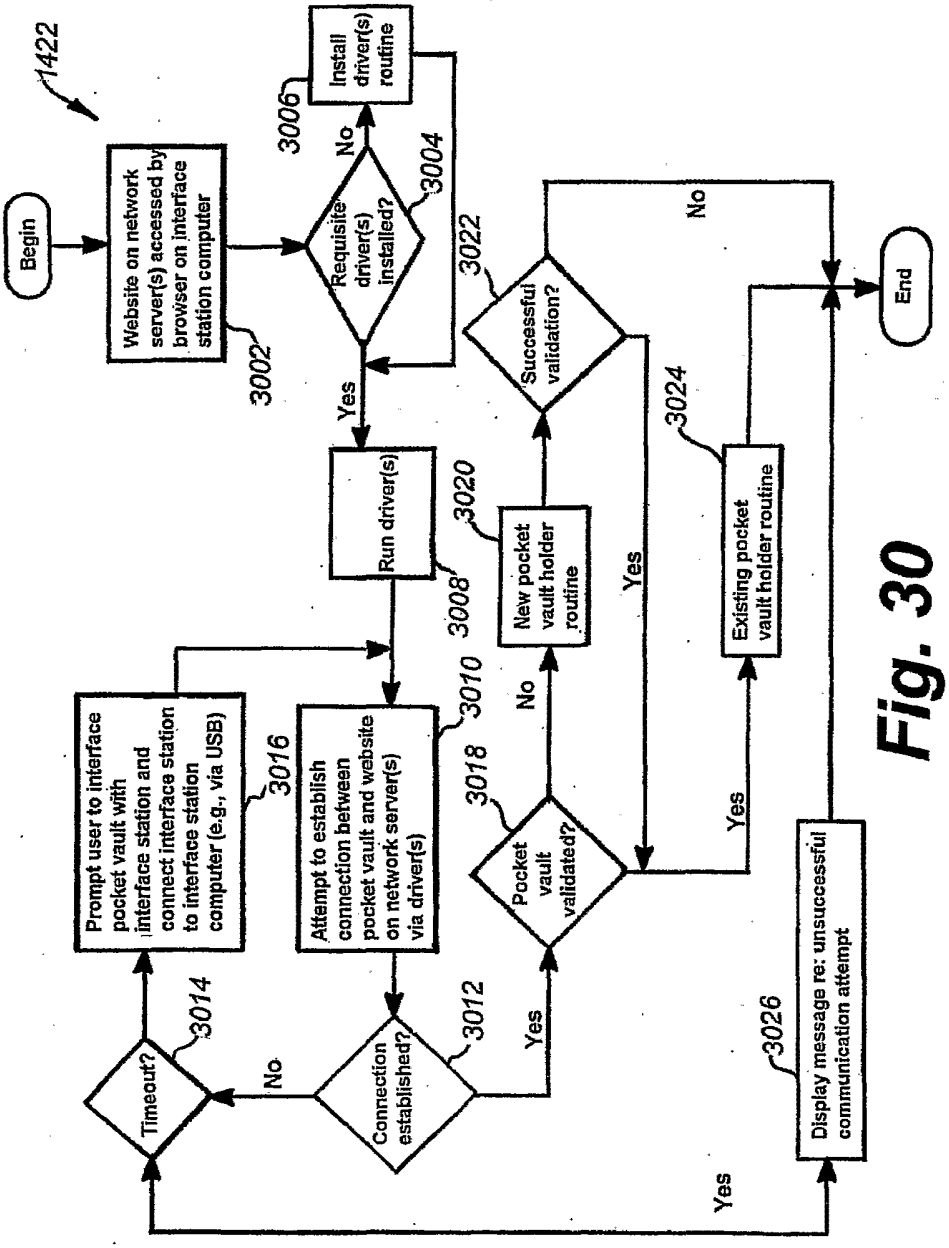

1422
Begin
Website on network server(s) accessed by browser on interface station computer
3002
Requisite driver(s) installed?
3004
No
Install driver(s) routine
3006
Yes
Run driver(s)
3008
Prompt user to interface pocket vault with interface station and connect interface station to interface station computer (e.g., via USB)
3016
Attempt to establish connection between pocket vault and website on network server(s) via driver(s)
3010
Timeout?
3014
No
Connection established?
3012
Yes
Pocket vault validated?
3018
No
New pocket vault holder routine
3020
Yes
Successful validation?
3022
No
Existing pocket vault holder routine
3024
Yes
Display message re: unsuccessful communication attempt
3026
Yes
End

Fig. 30

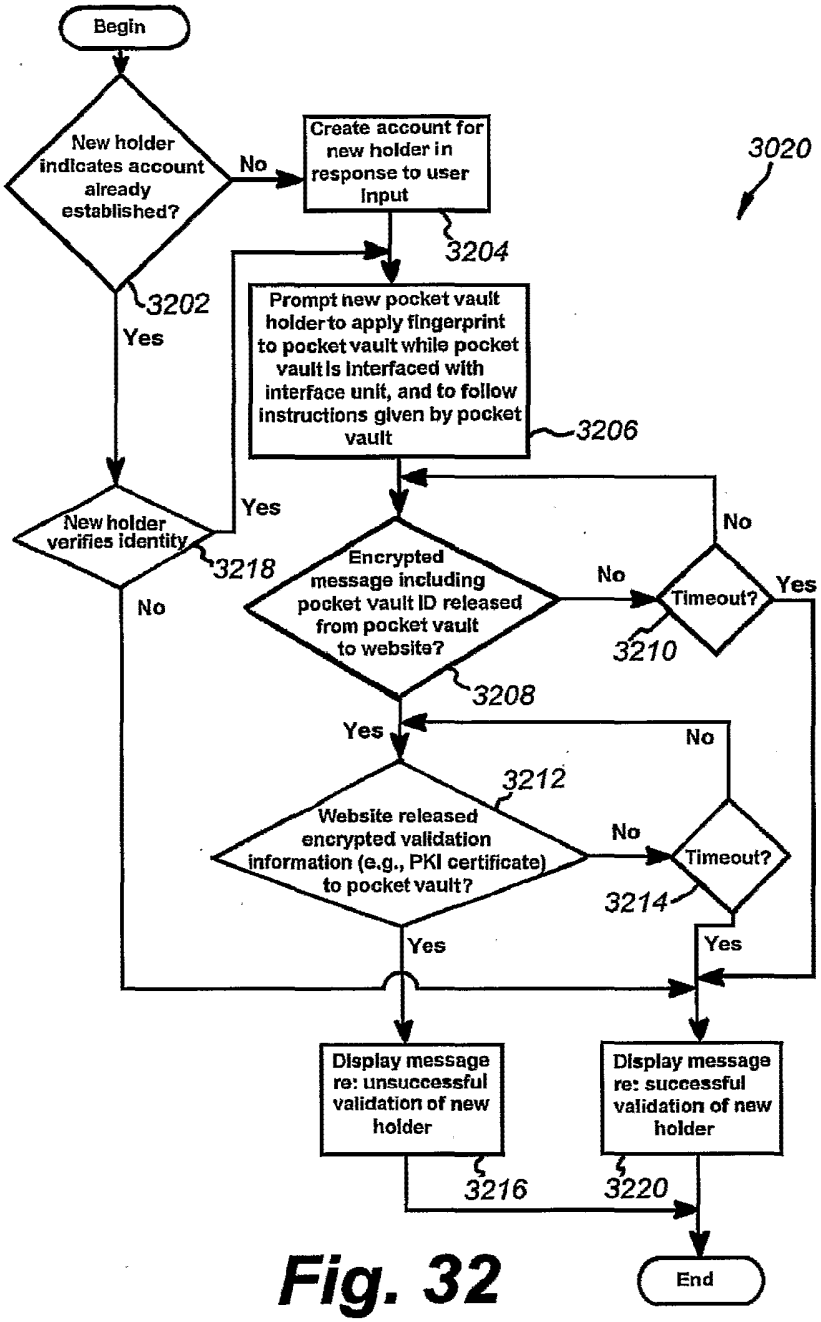

Begin
New holder indicates account already established?
No
Create account for new holder in response to user input
3204
3020
3202
Yes
Prompt new pocket vault holder to apply fingerprint to pocket vault while pocket vault is interfaced with interface unit, and to follow instructions given by pocket vault
3206
New holder verifies identity
Yes
3218
No
Encrypted message including pocket vault ID released from pocket vault to website?
No
Timeout?
Yes
No
3210
3208
Yes
No
3212
Website released encrypted validation information (e.g., PKI certificate) to pocket vault?
No
Timeout?
3214
Yes
Yes
Display message re: unsuccessful validation of new holder
Display message re: successful validation of new holder
3216
3220
End

Fig. 32

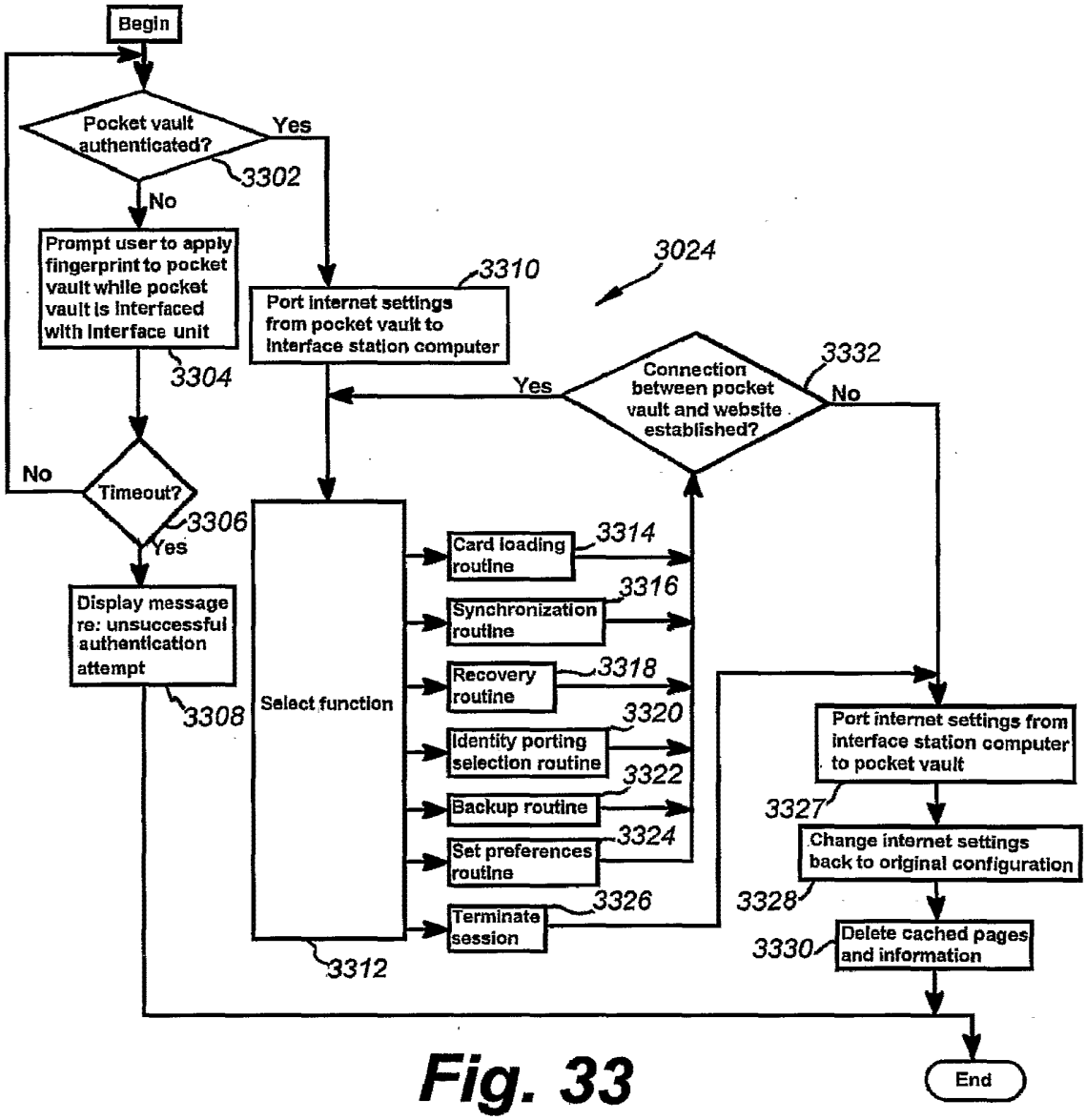

Begin
Pocket vault authenticated?
Yes
3302
No
Prompt user to apply fingerprint to pocket vault while pocket vault is interfaced with interface unit
3304
3310
Port internet settings from pocket vault to interface station computer
3024
Connection between pocket vault and website established?
3332
Yes
No
No
Timeout?
3306
Yes
Display message re: unsuccessful authentication attempt
3308
Select function
3312
Card loading routine
3314
Synchronization routine
3316
Recovery routine
3318
Identity porting selection routine
3320
Backup routine
3322
Set preferences routine
3324
Terminate session
3326
Port internet settings from interface station computer to pocket vault
3327
Change internet settings back to original configuration
3328
Delete cached pages and information
3330
End

Fig. 33

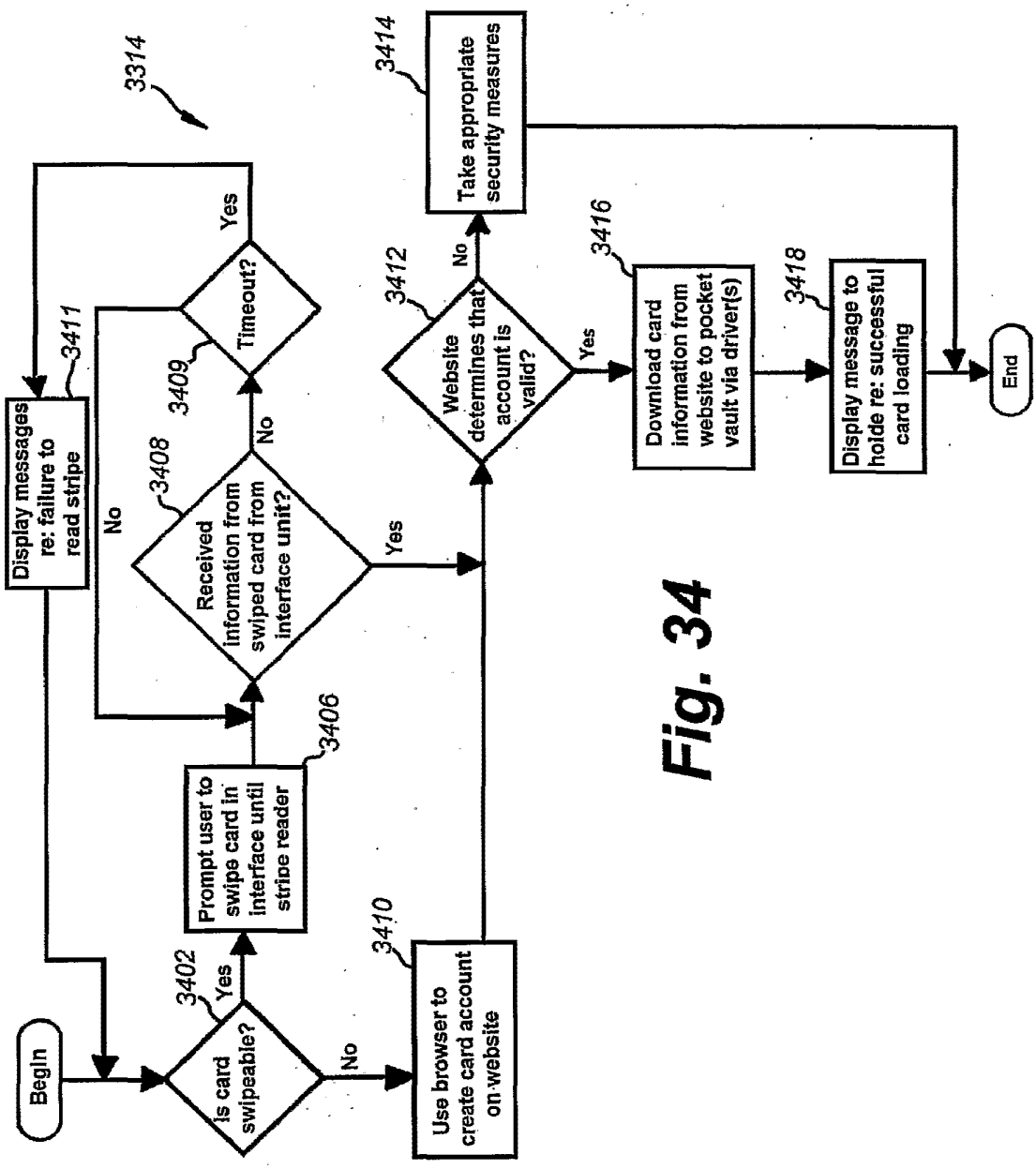

3314
Begin
Is card swipeable?
3402
Yes
No
Prompt user to swipe card in interface until stripe reader
3406
Use browser to create card account on website
3410
Received information from swiped card from interface unit?
3408
No
Yes
Timeout?
3409
Yes
No
Display messages re: failure to read stripe
3411
Website determines that account is valid?
3412
No
Yes
Take appropriate security measures
3414
Download card information from website to pocket vault via driver(s)
3416
Display message to holde re: successful card loading
3418
End

Fig. 34

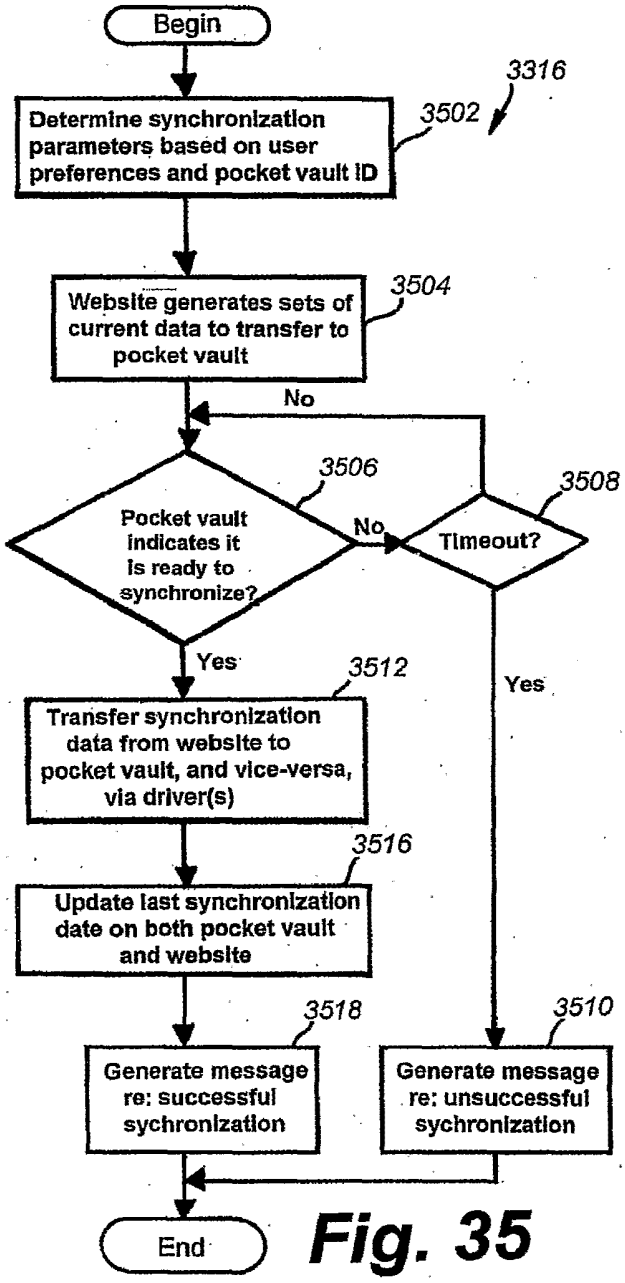

Begin
3316
Determine synchronization parameters based on user preferences and pocket vault ID
3502
Website generates sets of current data to transfer to pocket vault
3504
No
3506
Pocket vault indicates it is ready to synchronize?
No
3508
Timeout?
Yes
Yes
3512
Transfer synchronization data from website to pocket vault, and vice-versa, via driver(s)
3516
Update last synchronization date on both pocket vault and website
3518
Generate message re: successful sychronization
3510
Generate message re: unsuccessful sychronization
End

Fig. 35

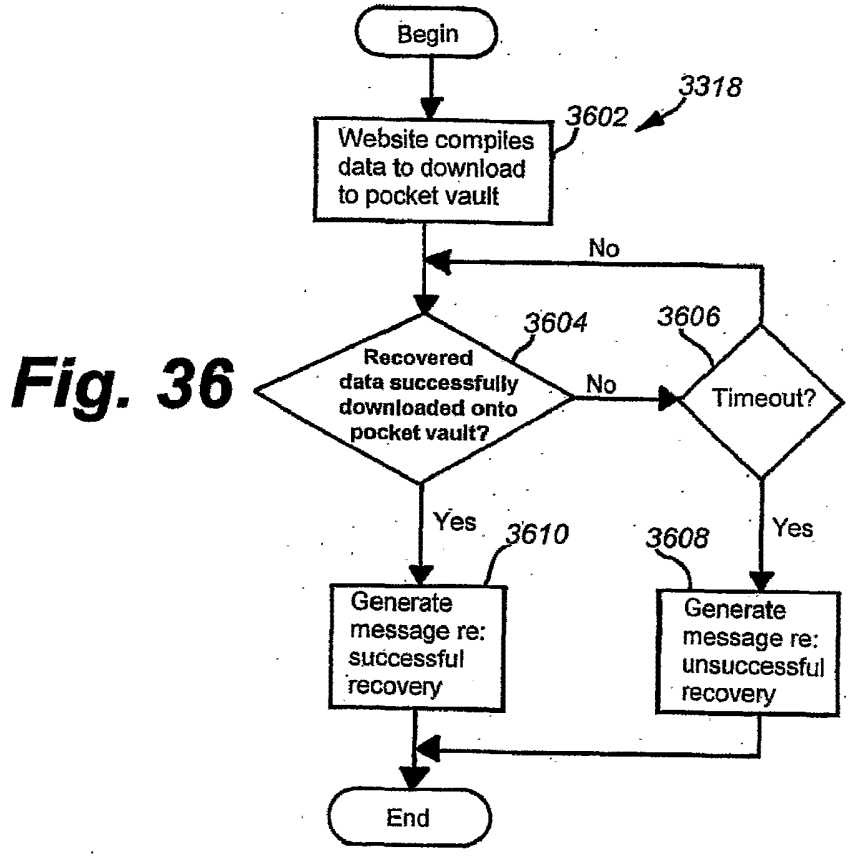

Begin
3318
3602
Website compiles data to download to pocket vault
No
3604
3606
Recovered data successfully downloaded onto pocket vault?
No
Timeout?
Yes
3610
3608
Yes
Generate message re: successful recovery
Generate message re: unsuccessful recovery
End

Fig. 36

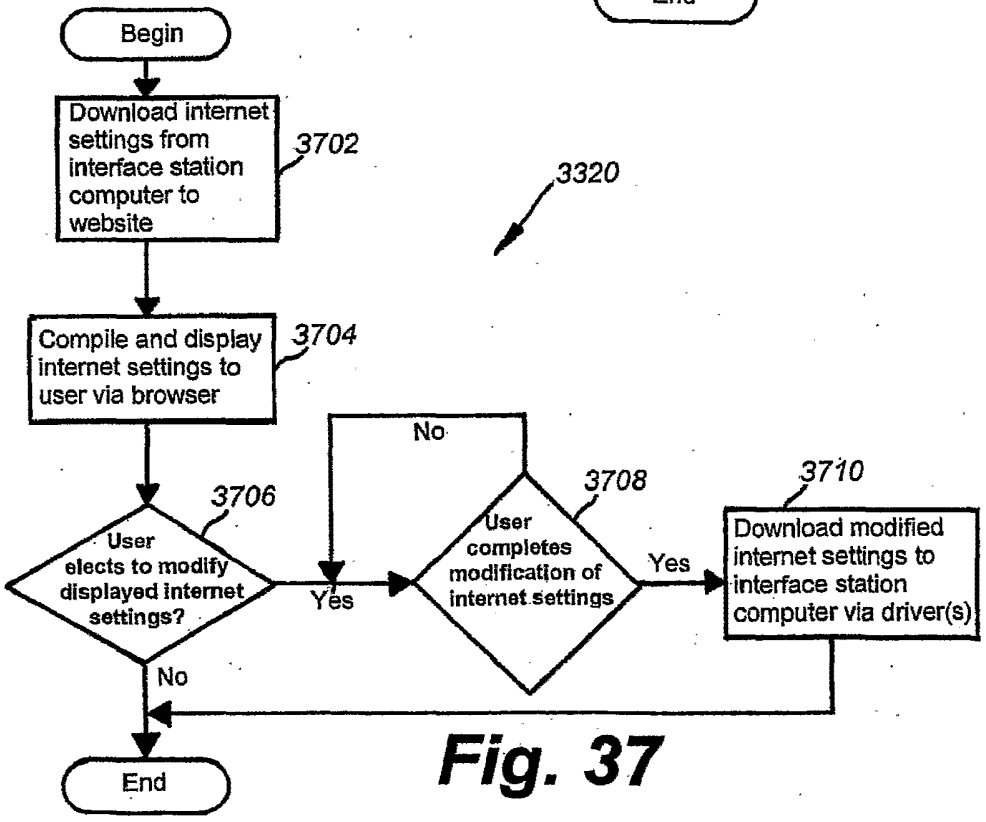

Begin
Download internet settings from interface station computer to website
3702
3320
Compile and display internet settings to user via browser
3704
No
3706
3708
3710
User elects to modify displayed internet settings?
Yes
User completes modification of internet settings
Yes
Download modified internet settings to interface station computer via driver(s)
No
End

Fig. 37

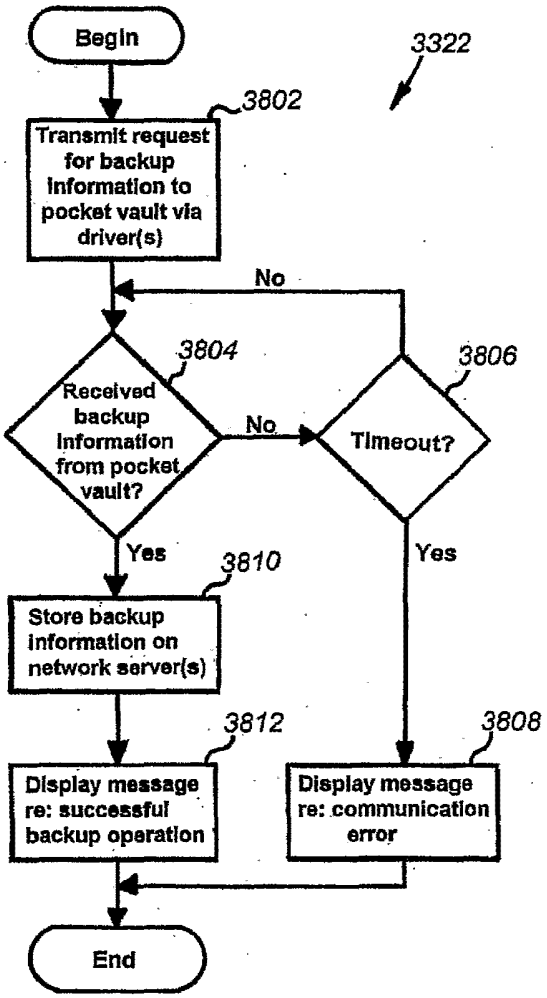

Begin
3322
3802
Transmit request for backup information to pocket vault via driver(s)
No
3804
Received backup information from pocket vault?
No
3806
Timeout?
Yes
Yes
3810
Store backup information on network server(s)
3812
Display message re: successful backup operation
3808
Display message re: communication error
End

Fig. 38

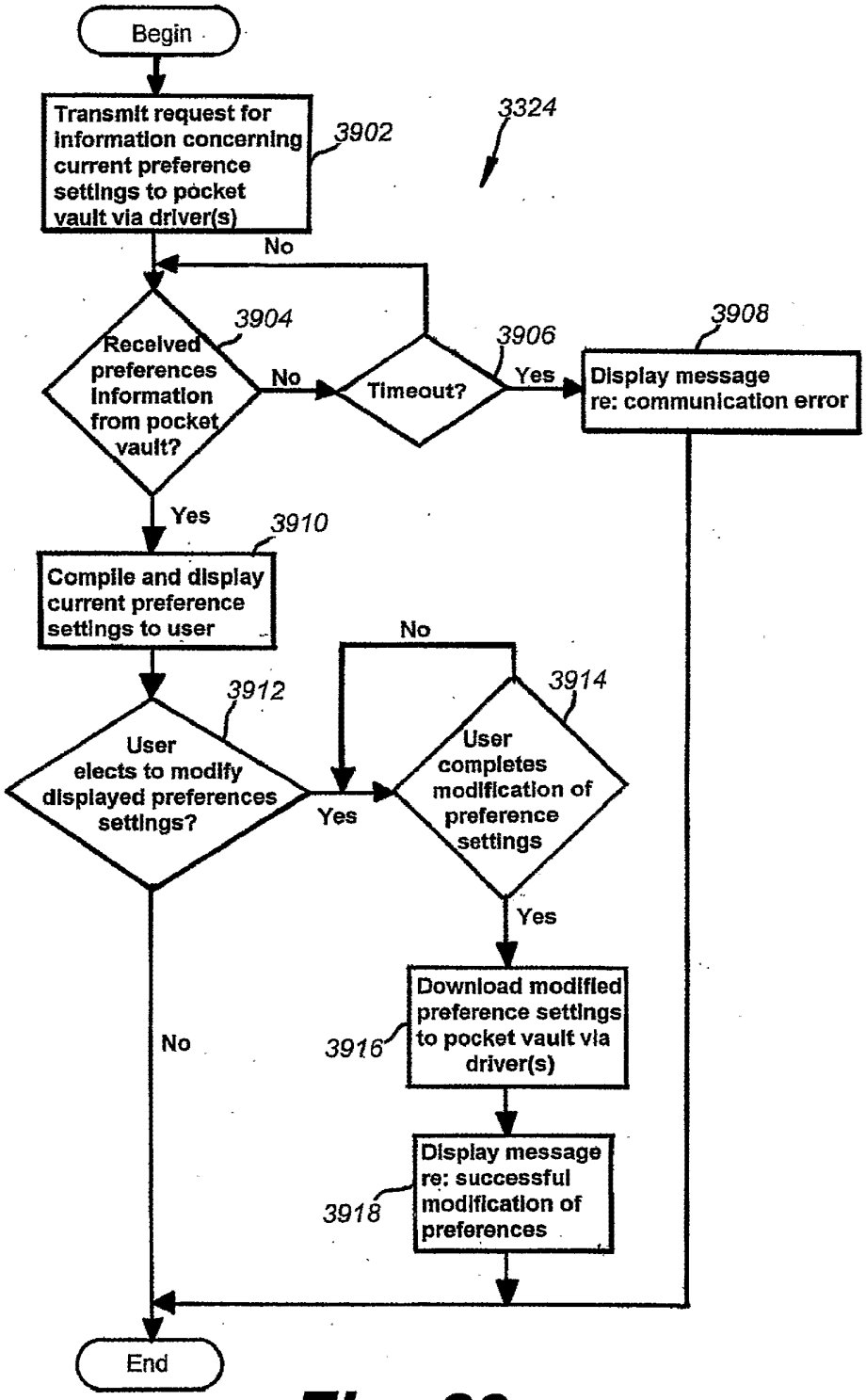

Begin
Transmit request for information concerning current preference settings to pocket vault via driver(s)
3902
3324
No
Received preferences information from pocket vault?
3904
No
Timeout?
3906
Yes
Display message re: communication error
3908
Yes
Compile and display current preference settings to user
3910
No
User elects to modify displayed preferences settings?
3912
Yes
User completes modification of preference settings
3914
Yes
No
Download modified preference settings to pocket vault via driver(s)
3916
Display message re: successful modification of preferences
3918
End

Fig. 39

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
18 September 2003 (18.09.2003)

PCT

(10) International Publication Number
WO 03/077473 A1

(51) International Patent Classification[7]: H04L 12/28, G07F 19/00

(21) International Application Number: PCT/DK03/00163

(22) International Filing Date: 13 March 2003 (13.03.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PA 2002 00387 13 March 2002 (13.03.2002) DK

(71) Applicant *(for all designated States except US)*: **BEAMTRUST A/S** [DK/DK]; Borupvang 1A, DK-2750 Ballerup (DK).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **ANDERSSON, Sten** [SE/SE]; Bryggaregatan 12, S-227 36 Lund (SE). **KAARLE, Peter** [SE/SE]; Lackes gränd 7, S-244 95 Furulund (SE). **KAPNOULA, Anna** [SE/SE]; Västra Stationstorget 14, S-222 37 Lund (SE). **ELGAARD, Robert** [DK/DK]; Stænget 11, DK-2820 Gentofte (DK).

(74) Agent: **ZACCO DENMARK A/S**; Hans Bekkevolds Allé 7, DK-2900 Hellerup (DK).

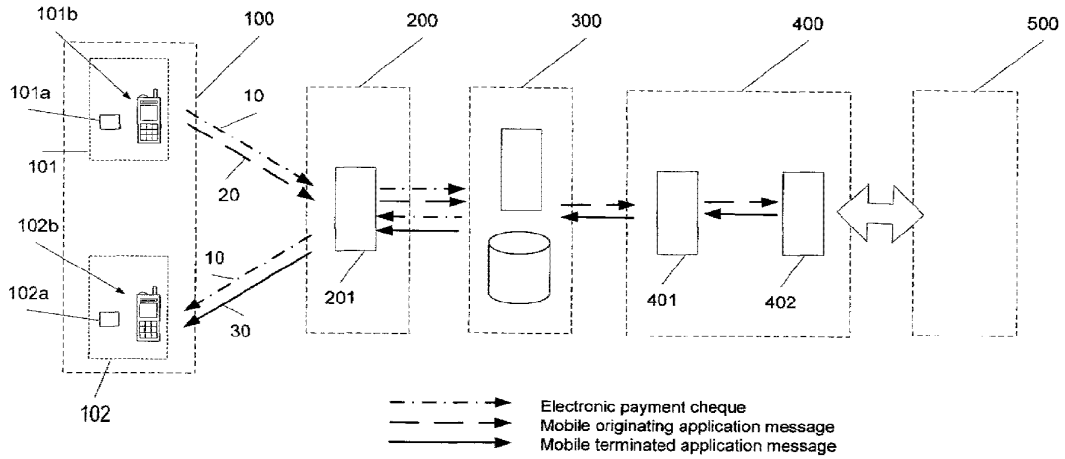
(81) Designated States *(national)*: AE, AG, AL, AM, AT (utility model), AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ (utility model), CZ, DE (utility model), DE, DK (utility model), DK, DM, DZ, EC, EE (utility model), EE, ES, FI (utility model), FI, GB, GD, GE, GH, GM, HR, HU, ID, 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 (utility model), SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, 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, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, 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: A METHOD OF PROCESSING AN ELECTRONIC PAYMENT CHEQUE



(57) Abstract: The invention relates to processing an electronic payment cheque that relates to a transfer of an amount of money from an account of a first user in a first banking institute to an account of a second user in a second banking institute, which processing includes generating digital signatures by means of asymmetric encryption. The method comprises the following steps: • in a first SIM card, creating an electronic payment cheque and signing the electronic payment cheque with a first signature; • transmitting the signed electronic payment cheque to a second SIM card in a second mobile equipment of the second user; • in the second SIM card, additionally signing the electronic payment cheque with a second signature; • transmitting the thus signed electronic payment cheque to subsequently initiate a deposit of the amount of money in the electronic payment cheque into the account of the second user.

WO 03/077473 A1

A method of processing an electronic payment cheque

This invention relates to a method of processing an electronic payment cheque that relates to a transfer of an amount of money from an account of a first user in a first banking institute to an account of a second user in a second banking institute, which processing includes generating digital signatures by means of asymmetric encryption using an asymmetric key pair comprising a private key and a public key.

A plurality of payment means are common today, such as bank notes and coins, cheques, money transfers from one bank account to another, credit cards, debit cards, giro transfer forms, etc. Some of these payment means are more suitable for transferring money from one person to another than others. The security of a money transfer is important; some persons do not want to carry big cash amounts, everybody prefers a security that a money transfer via a bank account or a giro account reaches the rightful receiver and when a payment means has an inherent protection against utilization, if unlawfully acquired, this is favoured.

Regarding money transfers, a solution which provides a secure and simple way of transferring money electronically from one person to another is desirable, for instance an electronic substitute of a cheque.

US patent 5,677,955 describes a computer-based electronic instrument that can comprise an electronic substitute of a cheque. It is described, that the electronic instrument can be transferred from one computer to another and can relate to the transferral of funds from an account of a payer to an account of a payee. The electronic instrument can be signed by means of an electronic signature using asymmetric key cryptography, and by receipt of the electronic substitute of a cheque, the payee can deposit the cheque at his bank by means of the internet and/or e-mails.

Even though the electronic substitute of a cheque can be stored on a portable PCMCIA card, the use of the electronic substitute of a cheque is not mobile as such, in that it is limited to use in computers/PC's. Moreover, the electronic substitute of a cheque might be cumbersome to use in that the requirements for the information included are relatively high.

It would be desirable to be able to use an electronic substitute of a cheque in a mobile telephone for a number of reasons, viz. the inherent mobility of mobile telephones, the low power consumption and the fact, that many mobile telephones are substantially always turned on. The use of electronic substitutes of cheques has yet not been carried into effect on mobile telephones because the high security, that is necessary in connection with any transferral of money, including a transferral of a electronic substitute of a cheque, has not yet been obtainable.

Therefore there is a need for a secure method to transfer an electronic substitute of a cheque from a mobile telephone to another mobile telephone and/or to a bank.

The above and other objects are reached when the method mentioned in the opening paragraph is characterised in that the method comprises the steps of in a first SIM card of the first user, creating an electronic payment cheque and signing the electronic payment cheque with a first signature generated by means of a first private key of a first asymmetric key pair, which first private key resides on the first SIM card hosted by the first mobile equipment; via a first mobile equipment hosting the SIM card of the first user, transmitting the signed electronic payment cheque to a second SIM card hosted in a second mobile equipment of the second user; in the second SIM card, signing the electronic payment cheque, which has been signed with a first signature, with an additional second signature generated on the second SIM card, by means of a second private key of a second asymmetric key pair, which second private key resides on the second SIM card hosted by the second mobile equipment; transmitting the electronic payment cheque signed

with the first and the second digital signatures from the second mobile station to a the central hub, which central hub is in communication with the first and the second banking institutes, and in the central hub, initiating a deposit of the amount of money in the electronic payment cheque into the account of the second user by initialising a verification of the second signature at the banking institution of the second user and a verification of the first signature at the banking institution of the first user.

When the creation and signing of the electronic payment cheque is performed on a SIM-card and the signing of a received electronic payment cheque for depositing/withdrawal thereof also is performed on SIM-card, a high level of security is obtained, because the interface between a SIM-card and a mobile equipment hosting it inherently limits the access to data on the SIM-card. Examples of the digital mobile telephone system used can be the Global System for Mobile communication (GSM) or Digital-American Mobile Phone Service (D-AMPS).

Preferably, the first and the second private key are generated on the first and the second SIM card, respectively, in the method according to the invention. When the private keys are generated on a SIM card and never have been exposed outside the SIM card, they are tamperproof.

In a preferred embodiment, the transmittal of the signed electronic payment cheque from the first mobile equipment hosting the SIM card of the first user to the second SIM card hosted in a second mobile equipment of the second user is performed via a digital mobile telephone system. In another preferred embodiment, the signed payment cheque is transmitted as a Short Message by means of IR, Bluetooth or Wi-Fi standards.

According to a preferred embodiment of the method, creating an electronic payment cheque comprises indicating a telephone number associated to the second SIM card, an amount to be transferred and an account index to the account, wherefrom the amount should be withdrawn. Thereby, the user of

the first mobile equipment, i.e. the issuer of an electronic payment cheque, need only know the telephone number of the receiver of the cheque, i.e. the user of the second mobile equipment, the amount he/she wants to transfer to the receiver and from which account he/she wants to withdraw the money. The method supports the possibility that the issuer of the electronic payment cheque has a plurality of accounts to choose to withdraw money from, and preferably a default account is set, from which the money is withdrawn if the user do not change this setting.

When the signed payment cheque is transmitted as a Short Message by means of the Short Message Service system over the GSM system, the method provides a cheap, fast and simple way of money transfer.

Preferably, the method further comprises via the first mobile equipment, prompting the first user to confirm creation of an electronic payment cheque, which prompting is initiated at the first SIM card hosted by the first mobile equipment. Hereby, it is avoided that money transfers are generated unintentionally. Preferably, the conformation of the creation of the electronic payment cheque comprises entering of a PIN-RSA number. The PIN-RSA number is a PIN code of 4 digits, which is used to get access to the key files on the SIM card.

According to the invention, the encrypted electronic payment cheque is transmitted via a message proxy and preferably, the encrypted electronic payment cheque proxy is converted to an SMS Point-to-point data download message, which subsequently is transmitted to the second SIM card hosted by the second mobile equipment. The message proxy is an integrated part of the central hub.

The message proxy in the central hub is suitable for sending application specific messages from a banking institute via a bank application, typically also hosted in the BDC, to SIM cards hosted in mobile equipment. A BDC domain may consist of several Bank domains, i.e. several banks that are

linked to the service of the BDC domain and are using the same BDC for processing of the transactions. The BDC domain can be divided into one BDC and several bank areas. The BDC is responsible for hosting some of the functionality that might be common between banks e.g. the Internet bank(s).

The other claims describe other preferred embodiments of the invention.

The term "mobile telephone" or "mobile phone" is used synonymous with "mobile station" and is used to define a mobile phone, which is divided in the two logical units: "mobile equipment" and "Subscriber Identity Module (SIM)". The mobile equipment has all the functions for radio communication with the digital mobile telephone system. The mobile equipment together with the SIM thus equals the mobile station. Without the SIM, the mobile equipment is only able to perform emergency calls. The SIM card is a smart card that is used for storing of subscription related information.

The invention will be explained more fully below in connection with an example of a preferred embodiment and with reference to the drawing, in which:

fig. 1a and 1b show overviews of the parts performing the method of the invention,

fig. 2 is a diagram of the data flow between some of the parts performing the method of the invention, and

fig. 3a and 3b overviews of the digital signature calculation and the digital signature verification, respectively.

Throughout the figures, the same reference numbers refers to like elements.

Fig. 1a shows an example of an overview of the parts performing the method of the invention. The parts are shown hosted in a user's domain 100, an operator's domain 200, a central hub 300, a Bank Data processing Centre's (BDC domain) 400 and in a banking institute 500, respectively. Shown are to mobile telephones 101 and 102 operating in a digital mobile telephone system 100, whereof the mobile telephone 101 is an issuer of an electronic payment cheque and the mobile telephone102 is the receiver thereof. This digital mobile telephone system 100 could be the Global System for Mobile communication (GSM) or Digital-American Mobile Phone Service (D-AMPS).

Throughout this description, the term "receiver" is meant to denote the mobile telephone 102, to which an electronic payment cheque is sent, and the term "issuer" is meant to denote the mobile telephone 101, from which the electronic payment cheque is sent. However, the terms "receiver" and "issuer" can also denote the user of the mobile telephone 102, to which an electronic payment cheque is sent, and the user of the mobile telephone 101 from which the electronic payment cheque is sent, respectively.

As stated above, the term "mobile telephone" or "mobile phone" is used synonymous with "mobile station" and is used to define a mobile phone 101, 102, which is divided in the two logical units: "mobile equipment" 101b, 102b and "Subscriber Identity Module (SIM)" 101a, 102a. The mobile equipment 101b, 102b has all the functions for radio communication with the digital mobile telephone system. The mobile equipment 101b, 102b together with the SIM 101a, 102a thus equals the mobile station 101, 102 respectively. In this description, the applications for performing the method of the inventions are placed on the SIM card; for facilitate the reading of this description, this is not always stated explicitly.

To use the method of the invention, i.e. activate the applications, a user has to register at the banking institute 500, typically through an Internet Bank, which will be explained below. After registration the user receives a new SIM card 101a, 102a from an operator 200, where the user is a subscriber. This

SIM card 101a, 102a contains an application for supporting issuance and reception of electronic payment cheques according to the method of the invention. The SIM card 101a, 102a is preferably personalised to allow remote updates over the air (OTA). An activation procedure must be successfully executed before it is possible to use the service for performing the method according to the invention, and thereafter, the user can use the mobile equipment together with the customised SIM card 101a, 102a. The application on the SIM card 101a, 102a is responsible for signing electronic payment cheques and for the interaction with the user.

The OTA updates are performed by sending application specific messages from the Bank application 402 to the mobile phone 101, 102 via an SMS Gateway/Proxy 401 in the BDC's domain 400 and the operator's SMS-C 201. The application messages are transferred as user data within Short Messages and are transported between the mobile phone 101, 102 and the SMS-C 201 using mobile originated and mobile terminated short messages

The BDC domain 400 has an interface to the central hub 300 and thereby to the operator's GSM environment. The SMS gateway 401 is responsible for communication with the SMS-C 201 within the operator domain 200 via the central hub 300. The Bank application 402 within the BDC domain 400 communicates with the SMS Gateway/Proxy 401 using an XML interface. With this interface it is possible for the BDC 200 to request OTA updates of application information on the SIM card 101a, 102a. The XML interface includes the receiver's phone number and a string to be sent either as an ordinary text message or an application message destined for the SIM application. The XML documents are sent between the Bank application 402 and the SMS Gateway/Proxy 401 using the HTTP method POST.

The SMS Gateway/Proxy 401 also has a service listening for mobile originated messages. This service handle all messages from mobile phones 101, 102 (independent of whether it's a mobile originating request or a

response of a mobile terminated request) and delivers the messages as a XML document to the domain of the banking institute 500.

For information transmitted from the Bank application 402 to the SMS Gateway/Proxy 401, the Bank application 402 acts as an HTTP client and the SMS Gateway/Proxy 401 acts as an HTTP server. For information transmitted from the SMS Gateway/Proxy 401 to the Bank application 402, the reverse applies, i.e. the SMS Gateway/Proxy 401 acts as an HTTP client whereas the Bank application 402 acts as an HTTP server.

The information exchange, shown by arrows, between the issuer 101 and the receiver 102 of an electronic payment cheque is carried out over Short Message Service (SMS) with assistance from the central hub 300 and an SMS gateway/proxy server 401 in the BDC domain 400 of the issuer's bank and via an SMS centre SMS-C 201 in the operator's domain 200. The SMS gateway/proxy server 401 is supported by a bank application 302, which is in communication with the banking institute 500. The BDC domain 400 can be located within or in close proximity to the banking institute 500, but this is not necessary as long as the BDC domain 400 and the banking institute 500 are able to communicate.

The communication between the SMS Gateway/proxy 401, the central hub 300 and the SMS-C 201 is transparent to the Bank application 402. The SMS Gateway/proxy 401 within the BDC domain 400 is connected to the operator's SMS-C 201 using an SMS-C protocol, such as SMPP. The SMS-C 201 is responsible for sending short messages to the mobile phone upon request from the SMS Gateway/proxy 401 as well as forwarding short messages originated from the mobile phone to the SMS Gateway/proxy 401. The mobile originated short messages are addressed to a specific SME address, a so-called large account. The SMS-C maps the SME address to an address to the SMS Gateway/proxy 401 and forwards the message to the SMS Gateway/proxy 401 within the BDC domain 400. The sender of the message, i.e. the MSISDN of the mobile phone, must be transferred from the

SMS-C 201 to the SMS Gateway/proxy 401 for further delivery to the Bank application 402.

In the above, the abbreviation SME denotes "Short Message Entity", which is an entity capable of receiving and/or sending short messages. The SME can for instance be located in the mobile station or in a fixed network. The abbreviation MSISDN denotes the "Mobile Station International ISDN Number", which is the standard international telephone number used to identify a given subscriber. The number is based on the ITU-T (International Telecommunications Union-Telecommunication Standardization Sector) E.164 standard. Finally, the abbreviation SMPP denotes "short message peer to peer", where "Peer to peer" is a communications model in which each party has the same capabilities and either party can initiate a communication session.

The application messages are thus transferred as user data within short messages and are transported between the mobile phone and the SMS-C 201 using mobile originated and mobile terminated short messages. The SMS Gateway 401 also has a service listening for mobile originated messages. This service handle all messages from a mobile phone 101, 102 (independent of whether it's a mobile originating request or a response of a mobile terminated request) and delivers the messages as a XML document to the banking institute 500. The SMS gateway/proxy functionality has to be able to send a message, coded as an SMS Point-To-Point Data Download message, from one mobile phone to another.

The requirements on the SMS gateway/proxy 401 are explained closer in the following. The SMS gateway/proxy 401 must be able to cheque all messages originating from a mobile station 101, 102. Depending on the message type, the SMS gateway/proxy 401 should either route the message to the banking institute 500 or forward the message to another mobile phone 101, 102. The messages shown in fig. 1 from or to a mobile telephone includes the electronic payment cheque 10, the mobile originating application message 20

and the mobile terminated application message 30. Of course, Short Messages (SM) sent from one mobile telephone 101 to another 102 can in general comprise text messages; however, those are not shown in fig. 1 since they are not in the interest of the invention.

On messages sent from one mobile phone 101 and forwarded to another mobile phone 102. The SMS gateway/proxy 401 should perform the following:

- Take the phone number of the receiver 102 from the mobile originating application message 20 and put it in the SM header as the Destination Address.
- Take the Originating Address from the mobile originating SM header and put it in the application message as a parameter for the sender's (issuer's) phone number.
- Preferably, append the actual date from the gateway/proxy server to the application message as a parameter. Hereby the electronic payment cheque is provided with a cheque issue date providing the option that a cheque is valid for a limited time period set by the bank. A cheques' valid time can then be counted from the time the cheque is sent i.e. the date when it passes the SMS Gateway/proxy server 401 of the issuer's banking institute 500.
- Code the mobile terminated message as SMS Point-To-Point Data Download (SMS PP DD) messages. This enables the Mobile equipment to transparently forward the short messages to the SIM.

Fig. 1b shows the elements from fig. 1a in conjunction with the domain 250 of an operator of the receiver, a domain 350 of a Bank Data processing Centre (BDC domain) of the receiver of the electronic payment cheque and a banking institute 550 of the receiver, respectively. The operator's domain 250 comprises an SMS centre SMS-C 251, and the BDC domain 350 of the

receiver's banking institute comprises an SMS gateway/proxy server 351 and a bank application 352. Hollow arrows in fig. 1a and 1b indicate that some communication can take place, without specifying this communications further.

When a receiver 102 has received an electronic payment cheque, he/she can deposit it in a bank account in his banking institute 550. For this purpose, the receiver sends an SMS from the mobile telephone 102 to his/her banking institute 550 via the SMS-C 251, the hub 300, the SMS gateway/proxy server 451 and the bank application 452 to the banking institute 550. This SMS contains the electronic payment cheque 10 and a cheque deposit request 40. After receipt of the cheque deposit request 40, the banking institute 550 initiates a communication with the banking institute 500 of the issuer to carry a transfer of money indicated in the electronic payment cheque from the issuer's account to an account of the receiver into effect. The details of this communication are described below.

The receiver 102 has received the electronic payment cheque with the telephone number of the receiving mobile telephone 102, the amount to be transferred from the issuer to the receiver and the issuer account, from which the money should be withdrawn together with the digital signature generated by the application on the SIM of the mobile telephone 101; additionally the SMS gateway/proxy 301 automatically appends the MSISDN of the issuing mobile telephone 101. Thereby the issuer of the electronic payment cheque can be presented unambiguously to the receiving mobile telephone 102. The SMS gateway/proxy 301 also adds a date stamp, which provides an issue date to the electronic payment cheque.

The receiver initiates a signing of the electronic payment cheque with a second digital signature, and the electronic payment cheque, thus signed with the first and the second digital signatures is transmitted from the second mobile station 102 to the central hub 300. The hub 300 performs the following processing:

- Sends the part of the cheque, which is signed by the second user 102 to the banking institution 550 of the second user 102. The banking institution 550 of the second user 102 verifies the signature and, on basis of the GSM number and account index of the second user 102, returns the corresponding account number.

- The central hub 300 attaches the real account number received from the banking institute 550 of the second user 102 to the part of the transaction, which is signed by the first user 101. This data is sent to the banking institute 500 of the first user 101. The banking institute 500 of the first user verifies the signature from the first user and determines whether sufficient funds exist in the account indicated by the telephone number (e.g. the GSM number) and account index of the first user 101. If sufficient funds exist in the account of the first user 101, the banking institute 500 of the first user 101 initiates a transfer to the second user's account in the second banking institute 550. The banking institute 500 of the first user 101 sends a reply back to the central hub 300. If the reply is a reject, the central hub 300 sends a short message to both the first and the second user 101, 102 with information, that the transfer has been rejected. If the reply is an acknowledgement, the central hub 300 sends an application type SMS to the second user 102, which application type SMS erases the check from the SIM card of the second user 102.

No matter whether the reply is a reject or an acknowledgement of the transfer of money, the receiver of the electronic payment cheque is notified thereof substantially without delay. Likewise the receiver of an electronic payment cheque is notified of the reception substantially without delay from the receipt.

Even though only two users, BDC's, two banking institutes are shown, it should be understood, that substantially any number of users in the user

domain can perform the method of the invention. Moreover a plurality of BDC's, banking institutes, SMS centres could be used in the implementation of the invention.

The application on the SIM card of a user for implementing the method of the invention supports issuance of cheques from a plurality of accounts in different banking institutes; a user have activated the service for implementing the method in e.g. 5 different banks for use of a total of 10 accounts.

Fig. 2 is a diagram of the data flow between some of the parts performing the method of the invention. Fig. 2 shows that cheque issuer data 50 are sent from a mobile telephone 101 of the issuer a second mobile telephone 102 of the receiver of the electronic payment cheque. The cheque issuer data 50 includes at least the electronic payment cheque, the telephone number of the receiving mobile telephone 102, the amount to be transferred from the issuer to the receiver and the issuer account, from which the money should be withdrawn. The cheque issuer data also contains a digital signature generated by the application on the SIM of the mobile telephone 101. The cheque issuer data 50 have thus been confirmed and signed by the issuer before sending and is sent via SMS. The cheque issuer data 50 are sent via the SMS gateway/proxy 301 (not shown in fig. 2) of the issuer, which SMS gateway/proxy receives the SM, recodes and forwards it to the receiving mobile telephone 102.

When the receiver 102 wants to deposit a received cheque to a bank account, it can also be done via SMS. The receiver 102 enters the appropriate application on the SIM card of the mobile telephone 102 via the appropriate menu entry in the service menu and is presented with a list of all received cheques. In the next interactions the receiver 102 chooses a cheque that should be deposited and, if no default account is set, also chooses the account to which it should deposited, and he/she enters the

personal service PIN code, the PIN-RSA, to allow the transaction to be signed.

Before a cheque deposit request 51 is sent from the receiver 102, a summary of the collected information is displayed to the receiver 102. The information displayed is amount, account nickname, date and a reference number. The reference number shown is a transaction identifier concatenated with the signature identifier. The user confirms and digitally signs the summary and the cheque deposit request 51 is transmitted to the central hub 300. Thus, the cheque deposit request 51 includes both the signature of the receiver of the cheque and the signature of the issuer of the cheque.

The central hub 300 initiates a data communication 52 to the banking institution 550 of the second user 102. The central hub 300 sends the part of the cheque, which is signed by the second user 102 to the banking institution 550 of the second user 102 in the data transmission 52, and the banking institution 550 of the second user 102 verifies the signature and, on basis of the GSM number and account index of the second user 102, returns the corresponding account number to the central hub 300.

The central hub 300 attaches the real account number received from the banking institute 550 of the second user 102 to the part of the transaction, which is signed by the first user 101. This data is sent to the banking institute 500 of the first user 101 in a data transmission 53. The banking institute 500 of the first user verifies the signature from the first user and determines whether sufficient funds exist in the account indicated by the telephone number (e.g. the GSM number) and account index of the first user 101. If sufficient funds exist in the account of the first user 101, the banking institute 500 of the first user 101 initiates a transfer (not shown) to the second user's account in the second banking institute 550.

The banking institute 500 of the first user 101 sends a reply 54 back to the central hub 300. If the reply 54 is a reject, the central hub 300 sends a short

message 55, 56 to the first and the second user 101, 102, respectively, with information, that the transfer has been rejected. If the reply is an acknowledgement, the central hub 300 sends an application type SMS 55 to the second user 102, which application type SMS 55 erases the check from the SIM card of the second user 102.

The generation of digital signatures by means of asymmetric encryption using an asymmetric key pair comprising a private key and a public key is well known per se, but its use in connection with the invention will be described in the following with reference to fig. 3a and 3b.

Asymmetric encryption systems, or public key systems, use two different keys, a public key 4b and a private key 4a, for encryption and decryption. The two keys 4a, 4b are dependent on each other and form a personally unique key pair, but it is not possible to calculate one key from knowledge of the other. Either the public or the private key can be used for encryption. The decryption is then made with the corresponding key of the key pair. For example, a message encrypted with a recipient's public key can be decrypted only with the same recipient's private key. The RSA (Rivest, Shamir, Adleman) algorithm is today a de facto standard for public key systems.

Hash algorithms 2 are used to create a digital fingerprint, or a message digest of a certain piece of information. Even the slightest change in the original message document produces a completely different digital fingerprint. A MAC (Message Authentication Code) is a hashed message encrypted using a symmetric key. A MAC gives message integrity but not non-repudiation. SHA-1 is a commonly used hash algorithm. It produces a 20-byte message digest of any input message.

A digital signature is created in the following way:

- An original message 1 is hashed with a hash algorithm 2 (e.g. SHA-1) and the digital fingerprint 3 of the original message is created.

- The fingerprint 3 is encrypted with the sender's private key 4a.
- The result is a digital signature 5 that is unique for every combination of message 1 and private key 4a. The message 1 and the digital signature 5 form an entity 6.

Upon reception, the digital signature 5 is verified in the following way:

- The original message in the entity 6 containing the original message 1 and the digital signature 5 is run through the hash algorithm 2 that was used in creation of the digital signature 5, thereby providing a digital fingerprint 3'.
- The signature 5 is decrypted with the sender's public key 4b, providing a decrypted, digital fingerprint 3".
- The digital fingerprint 3' and the decrypted, digital fingerprint 3" are compared at 7. If they are identical, the digital signature 5 is valid.

Digital signatures provide the following:

- Authentication of the sender's identity.
- Assurance that any changes to the message will be noticed (integrity).
- Assurance that the sender can not deny sending the message (non-repudiation).

In the method of the invention, the concepts introduced above are used to create secure transactions.

During the activation process of the service for performing the method of the invention, which will be described below, an RSA key pair is generated on the SIM card. The private key is stored in a tamperproof area on the SIM card, and the public key is exported from the mobile phone to the server in the BDC domain. In return, the server sends its own public RSA key to the

mobile phone. All RSA keys (both end-user and BDC keys) have a 1024-bit modulus and a public exponent set to 2^16+1 (=65537).

In order for the server to be able to authenticate the sender of the public key, the user has previously received a One-Time-Password (OTP) from the server on a secure, separate channel (e.g. via Internet Bank). The application on the SIM card calculates a message digest using SHA-1. The input is a concatenated string of all the information sent in the message (including the public key) and the OTP. The generated message digest is 20 bytes, but it is truncated to the first 8 bytes to create an Authentication Code.

The public key together with the other information and the Authentication Code are exported to the BDC domain. The total length of the message will be 139 bytes (1 byte Message Type + 1 byte Protocol Version + 1 byte SIM Application Version + 128 bytes Public Key + 8 bytes Authentication Code), which can be sent in one SM.

The server can then calculate an Authentication Code in the same way on the known OTP and the received information. If a comparison with the received Authentication Code is successful, it can be assumed that the public key has not been corrupted during transfer and that it indeed originates from the user. If the public key of the user is accepted, the server sends the public key belonging to the BDC domain, which will be used for server authentication purposes in subsequent operations. The message contains a new Authentication Code, which makes it possible for the application on the SIM card to verify that the message is originated from the correct source. It also contains an BDC identifier BDC-ID, which is used by the phone to link the public key to the correct BDC (in a multiple BDC scenario). The Authentication Code is again the first 8 bytes of a message digest calculated using SHA-1. The input is a concatenated string of all the information sent in the message (including the public key) and the OTP.

The public key together with the other information and the Authentication Code are sent to the mobile phone. The total length of the message will be 138 bytes (1 byte Message Type + 1 byte BDC-ID + 128 bytes Public Key + 8 bytes Authentication Code), which can be sent in one SM. The application on the SIM card can then calculate an Authentication Code in the same way on the known OTP and the received information. If the comparison with the received Authentication Code is successful, it can be assumed that the public key has not been corrupted during transfer and that it indeed originates from the BDC.

In order for the mobile phone to be able to trust OTA updates and requests from the BDC domain, a mechanism for server authentication is needed.
All information in messages from the server is encrypted using RSA with the BDC's private key according to Public Key Cryptography Standards. This creates a signature, which makes it possible for the application on the SIM card to perform server authentication upon reception of the message. In addition to the application information, the signed message contains the Message Type, the BDC identifier and a sequence number.

Note, that the Message Type and the BDC identifier are also sent unencrypted to the mobile phone, as they are needed by the SIM application before the signed message has been verified (decrypted). The Message Type is used to determine how the message should be handled. The BDC identifier is used to select the public key that should be used to decrypt the message.

The sequence number is a 3-byte integer generated by the BDC, which must be incremented for each new operation that the BDC requests towards a specific user, i.e. a separate counter is used for each user.
Before the encryption operation, the information has to be padded to 128 bytes. Since no hash of the message is calculated, the hash algorithm

identifier will not be included. Basically, the padding is performed in the following way:

- Construct a padding string consisting of (128-[length in bytes of data to sign]-3) octets with the hexadecimal value FF.
- Concatenate the padding string, the message to be signed, and delimiters to form the padded message

The padded message is then signed by the BDC by encrypting the information with the private key of the BDC.When the message is received, the SIM application performs the following steps:

- The message is decrypted using RSA with the BDC's public key. The BDC-D is used to select which public key is used to decrypt the message.
- The padding is checked to verify that the information has not been changed after it was signed, and then removed to recover the signed data. For additional security, the BDC-ID and the Message Type in the signed message can also be compared to the BDC-ID and the Message Type that were sent unencrypted to verify that the information has not been changed.
- The sequence number is compared to the sequence number received with the latest OTA request, in order to prevent replay attempts. The number must be incremented by the server for each new OTA request.

Mobile transactions initiated by the user are signed and can be listed as follows:

- Issue cheque (via SMS)
- Deposit cheque (via SMS)

The transactions are signed using RSA according to Public Key Cryptography Standards.

Below, the parameters and their order as they are signed during the transaction are outlined. The SHA-1 hash is calculated on the following concatenated data in each transaction.

Issue cheque

MSISDN_receiver	(20 bytes)
BDCID_issuer	(1 byte)
AccountID_issuer	(1 byte)
ChequeAmount	(15 bytes)
ChequeID	(3 bytes)

The format on the telephone number of the receiver, MSISDN_receiver, when signed is the complete international phone number, entered by the user, without the leading '+' or "00" string.

Deposit cheque

BDCID_receiver	(1 byte)
AccountID_receiver	(1 byte)
SignID	(3 bytes)
ChequeIssueDate	(8 bytes)
Signature_issuer	(128 bytes)

In the transaction summary a 7-digit reference number (RefNo) is displayed to the user. The RefNo is usually a 4-digit transaction identifier (TrxID) concatenated with the user's 3-digit signature identifier (SignID). During a deposit cheque transaction, however, no interaction with a pay-box takes place and no TrxID can therefore be received. To keep the RefNo in a uniform format to the user the TrxID is in this operation replaced with a dummy value ("0000") which is not signed.

In signature calculation, the 20-byte result of the SHA-1 operation above is padded to 128 bytes and encrypted using RSA with the user's private key.

The padding is done according to the EMSA-PKCS1-v1_5 encoding operation. Basically, the padding is performed in the following way:

- Hash the message using SHA-1.
- Construct a SHA-1 hash algorithm identifier using DER (Distinguished Encoding Rules). This results in the following octet string:

  30 21 30 09 06 05 2b 0e 03 02 1a 05 00 04 14
- Construct a padding string consisting of 90 octets with the hexadecimal value FF.
- Concatenate the padding string, the algorithm identifier, the hashed message, and delimiters to form the padded message:

00 || 01 || FF FF [...86xFF...] FF FF || 00 || 30 21 30 09 06 05 2b 0e 03 02 1a 05 00 04 14 || [hashed message]

The signature verification is done in the following way:

- Hash the original transaction using SHA-1 and apply the padding described above.
- Decrypt the signature using RSA and the user's public key.
- Compare the hashed and padded transaction with the decrypted signature. If they match, the signature is valid.

The user registration, i.e. the activation of the applications on the SIM card, will be described below. The registration described takes place via an Internet bank. It is presumed, that the user has received a new SIM card from the operator and has been instructed to activate the service for performing the method of the invention through the Internet Bank. Therefore, it is implicitly presumed, that the user is a registered user of an Internet Bank and that a trusted relationship thus already exists between the user and the bank. Moreover it is presumed, that the user has registered to the service for performing the method of the invention via the Internet Bank, and that the bank thereafter has sent a request to an operator for issuing and distributing

a new SIM card supporting the applications for performing the method of the invention to the user. Moreover, it is presumed, that the mobile telephone is switched on and the new SIM card is inserted.

The user selects a menu choice in the Internet Bank for activation of the service for performing the method of the invention. Then an 8-digit One-Time-Password (OTP) is displayed to the user on the screen. This information is used in the SIM application to provide user authentication and initiate the key generation. The user is instructed to select the menu choice for activation of the service for performing the method of the invention on the mobile phone.

The user selects an option "Service activation" in the menu on the mobile phone and enters the OTP. Entering the OTP triggers generation of the RSA key pair on the SIM card. The private key is stored in a tamperproof location on the SIM card. The application on the SIM card calculates an Authentication Code. The input is all information in the message, i.e. the message type, the OTA protocol version, the SIM application version, and the public key of the user, concatenated with the OTP. The generated 8-byte Authentication Code is then sent together with the other parameters in a SM to the BDC domain.

Note that an SME address (phone number) is needed on the SIM card to send messages to the BDC domain. The SME address can be pre-configured on the SIM card, but in a multiple BDC environment, the SME address may preferably be displayed to the user on the computer screen together with the OTP, and then entered into the mobile phone after the OTP.

Before the public key is accepted for use within the BDC domain, the Authentication Code received from the mobile phone is compared with an Authentication Code calculated locally in the BDC domain on the same parameters. If the comparison is successful the public key is stored.

If the public key of the user is accepted, the BDC domain exports its own public key, which will be used for server authentication purposes in subsequent operations. The message contains a new Authentication Code, which makes it possible for the application on the SIM card to verify that the message is originated from the correct source. It also contains the BDC-ID, which is used by the phone to link the public key to the correct BDC (in a multiple BDC scenario).

The Authentication Code is calculated, and the input is all information in the message, i.e. the message type, the BDCID, and the public key of the BDC, concatenated with the OTP. The generated 8-byte Authentication Code is then sent together with the other parameters in a SM to the mobile phone.

When the message is received, the application on the SIM card validates the Authentication Code by comparing it with an Authentication Code calculated locally in the mobile phone on the same parameters. If the validation is successful, the public key is stored and the BDC domain is notified of the result.

The BDC domain then sends a message to the mobile phone containing the information required for configuration of the application on the SIM card. The information package is signed (encrypted) with the BDC's private key before it is sent to the mobile phone. This makes it possible for the SIM application to perform server authentication upon reception of the message.

In addition to the application information, the signed message contains the Message Type, the BDC-ID and a sequence number. The Message Type and the BDC-ID are also sent unencrypted, as the SIM application needs these parameters in order to handle the message. The message is then signed**Error! Reference source not found.**.

When the message is received, the SIM application verifies the signed message and checks the sequence number. The BDC-ID is used to select the public key that should be used to verify the message.

If the validation is successful, the application data is stored and the BDC domain is notified of the result. The sequence number received in the request from the BDC is returned in the response and could be used on the server side to link the result to the corresponding request.

The user is requested to select a PIN code of 4 digits, which will be used to get access to the key files on the SIM card. This PIN code is referred to as PIN-RSA herein. Finally, the user is informed that the service for performing the method of the invention has been activated through a text message on the mobile phone display.

A useful functionality that can be provided by the central hub is to handle a cheque book via a web server. When a user sends a cheque to another user, the transmission passes through the central hub and the SMS-server. When the central hub registers the cheque, it can send a "Cheque issued" message to the web server. The "cheque issued" message contains the telephone number of the issuer and of the receiver, account index, cheque identification, the amount of money to be transferred and the date. The web server writes these data in a cheque book table.

When the receiver of an electronic payment cheque deposits the cheque, this will be performed via the central hub. When the central hub receives an acknowledgement of the transfer of money from the issuer's banking institute, the central hub sends a "cheque cleared" message to the web server. This "cheque cleared" message contains cheque identification, the telephone number of the issuer and of the receiver, the amount of money to be transferred and the date. The web server puts this cheque into a "cheque cleared" table. Hereby, the issuer as well as the receiver automatically has an updated cheque book of issued and received cheques.

Via a web interface a user (i.e. an issuer and/or a receiver) can connect to the web server and see all issued cheques. For instance, the following five possibilities might exist: "All cheques", "cleared cheques", "issued cheques", "received cheques" and "cashed cheques".

"All cheques" shows a list of all the cheques the user have issued and/or received with the status thereof (deposited or not deposited at an account in a banking institute). "Cleared cheques" shows a list of the cheques that the user has sent and which have been deposited by the receiver(s) thereof. "Issued cheques" shows a list of the cheques that the user has sent but which have not been deposited yet by the receiver(s) thereof. "Received cheques" shows a list of the cheques that the user has received but which have not yet been deposited and "Cashed cheques" shows a list of the cheques that the user has received and which have been deposited at an

account in a banking institute. The facility "Cleared cheques" provides the user with the possibility to determine whether a cheque has been deposited, which could be of relevance in the situation of a receiver asserting not to have received the cheque. If a receiver asserts not to have received a sent cheque, the cheque can be retransmitted. This re-transmittal is secure, in that the banking institute would reject any duplicate cheques.

Moreover, this cheque book service can include general filtering mechanisms such that a user can choose only to see cheques issued and/or received within a chosen time interval, from and/or to chosen telephone numbers, etc.

A cheque will expire after a specified number of days. The web sever can notify a user who has an "un-cashed" cheque, when the expiration date thereof is approaching by means of a Short Message.

Above, it has been explained that messages can be sent as Short Messages via the SMS service. However, due to the large amount of information and the signature in a cheque, a cheque issued and sent from an issuer to a receiver has to be sent as two short messages. The signature of the first user is split into two parts and the cheque is then sent as two SM, with one part of the signature in each. To be able to associate the messages again on the receiver's side each message must contain a reference to the other part of the message; this parameter is called the MessageReference and is a one-byte counter that is unique for each user. Both messages must include the phone number (MSISDN) of the receiver to allow the SMS proxy to forward the messages to the receiver. The second part of the cheque sent from the issuer to the receiver, containing the second part of the signature.

As explained in detail above, the deposit of a cheque issued by an issuer and sent to a receiver at the banking institute of the receiver can be started up by means of Short Messages sent from the receiver. Again, due to the large amount of information and the need to include both the issuer's and the receiver's signatures, the request message has to be sent as three short

messages. The first SM contains the cheque information and the next two short messages contain the signatures of the receiver and the issuer respectively. To be able to associate the messages again on the receiver's side each message must contain a reference to the other parts of the message; this parameter is called the MessageReference and is a one-byte counter that is unique for each user.

It is well known to use mobile telephones provided with IrDA, fast IrDA or Bluetooth facilities to withdraw money from Automatic Teller Machines ATM. If the electronic payment cheque service is implemented in the SIM card of a mobile telephone with the IrDA, fast IrDA or Bluetooth facility, the mobile telephone can be used to withdraw the amount of money in the electronic payment cheque by means of an ATM. Moreover, the user could choose to withdraw some of the amount of money indicated in the electronic payment cheque from the ATM and deposit the remaining part of the amount into an account.

In general, it should be noted that point-to-point communication between a mobile station (mobile telephone) and another mobile station also could be in accordance with the IrDA or fast IrDa standard, the Bluetooth standard, Wi-Fi standard and/or any other near-range communication standard

CLAIMS:

1. A method of processing an electronic payment cheque that relates to a transfer of an amount of money from an account of a first user in a first banking institute (500) to an account of a second user in a second banking institute (550), which processing includes generating digital signatures by means of asymmetric encryption using an asymmetric key pair comprising a private key and a public key, characterized in that, the method comprises the following steps:

in a first SIM card (101a) of the first user, creating an electronic payment cheque and signing the electronic payment cheque with a first signature generated by means of a first private key of a first asymmetric key pair, which first private key resides on the first SIM card (101a) hosted by a first mobile equipment (101b) ,

via the first mobile equipment (101b) hosting the SIM card (101a) of the first user, transmitting the signed electronic payment cheque to a second SIM card (102a) hosted in a second mobile equipment (102b) of the second user,

in the second SIM card (102a), signing the electronic payment cheque, which has been signed with the first signature, with an additional second signature generated on the second SIM card (102a) by means of a second private key of a second asymmetric key pair, which second private key resides on the second SIM card (102a) hosted by the second mobile equipment (102b),

transmitting the electronic payment cheque signed with the first and the second digital signatures from the second mobile equipment (102b) to a central hub (300), which central hub (300) is in communication with the first and the second banking institutes (500, 550),

in the central hub (300), initiating a deposit of the amount of money in the electronic payment cheque into the account of the second user by initialising a verification of the second signature at the banking institution (550) of the second user and a verification of the first signature at the banking institution of the first user (500).

2. A method according to claim 1, wherein the first and the second private key are generated on the first and the second SIM card (101a, 102a), respectively.

3. Method according to claim 1, wherein the transmittal of the signed electronic payment cheque from the first mobile equipment (101b) hosting the SIM card (101a) of the first user to the second SIM card (102a) hosted in a second mobile equipment (102b) of the second user, is performed via a digital mobile telephone system.

4. A method according to any of the claims 1 to 3, wherein the signed payment cheque is transmitted as a Short Message by means of the Short Message Service system over the GSM system.

5. A method according to any of the claims 1 to 3, wherein the signed payment cheque is transmitted as a Short Message by means of Ir, Bluetooth or Wi-Fi standards.

6. A method according to any of the claims 1 to 5, wherein creating of an electronic payment cheque comprises indicating a telephone number associated to the second SIM card (102a), an amount to be transferred and an index to the account, wherefrom the amount should be withdrawn.

7. A method according to any of the claims 1 to 6, wherein the method further comprises:

via the first mobile equipment (101b), prompting the first user to confirm creation of an electronic payment cheque, which prompting is initiated at the first SIM card (101a) hosted by the first mobile equipment (101b).

8. A method according to claim 7, wherein the conformation comprises entering of a PIN-RSA number.

9. A method according to any of the claims 1 to 8, wherein the encrypted electronic payment cheque is transmitted via a message proxy in the central hub (300).

10. A method according to claim 9, wherein the encrypted electronic payment cheque at the message proxy is converted to an SMS Point-to-point data download message, which subsequently is transmitted to the second SIM card hosted by the second mobile equipment.

11. A method of issuing an electronic payment cheque that relates to a transfer of an amount of money from an account of a first user in a first banking institute (500) to an account of a second user in a second banking institute (550), which issuing includes generating a digital signature by means of asymmetric encryption using an asymmetric key pair comprising a private key and a public key, characterized in that, the method comprises the following steps:

in a first SIM card (101a) of the first user, creating an electronic payment cheque and signing the electronic payment cheque with a first signature generated by means of a first private key of a first asymmetric key pair, which first private key resides on the first SIM card (101a) hosted by a first mobile equipment (101b) ,

via the first mobile equipment (101b) hosting the SIM card (101a) of the first user, transmitting the signed electronic payment cheque to a second SIM card (102a) hosted in a second mobile equipment (102b) of the second user.

12. A method according to claim 11, wherein the first private key is generated on the first SIM card (101a).

13. Method according to claim 11 or 12, wherein the transmittal of the signed electronic payment cheque from the first mobile equipment (101b) hosting the SIM card (101a) of the first user to the second SIM card (102a) hosted in a second mobile equipment (102b) of the second user, is performed via a digital mobile telephone system.

14. A method according to any of the claims 11 to 13, wherein the signed payment cheque is transmitted as a Short Message by means of the Short Message Service system over the GSM system.

15. A method according to any of the claims 11 to 14, wherein the signed payment cheque is transmitted as a Short Message by means of Ir, Bluetooth or Wi-Fi standards.

16. A method according to any of the claims 11 to 15, wherein creating of an electronic payment cheque comprises indicating a telephone number associated to the second SIM card (102a), an amount to be transferred and an index to the account, wherefrom the amount should be withdrawn.

17. A method according to any of the claims 11 to 16, wherein the signed electronic payment cheque is transmitted via a message proxy.

18 A method according to claim 17 wherein the signed electronic payment cheque at the message proxy is converted to an SMS Point-to-point data download message, which subsequently is transmitted to the second SIM card (102a) hosted by the second mobile equipment (102b).

19. A method of depositing a received electronic payment cheque that relates to a transfer of an amount of money from an account of a first user in a first banking institute (500) to an account of a second user in a second banking

institute (550), which processing includes generating digital signatures by means of asymmetric encryption using an asymmetric key pair comprising a private key and a public key, characterized in that, the method comprises the following steps:

in the second SIM card (102a), signing the received electronic payment cheque, which has been signed with a first signature, with an additional second signature generated on the second SIM card (102a), by means of a second private key of a second asymmetric key pair, which second private key resides on the second SIM card (102a) hosted by the second mobile equipment (102b),

transmitting the electronic payment cheque signed with the first and the second digital signatures from the second mobile equipment (102b) to the central hub (300), which central hub (300) is in communication with the first and the second banking institutes (500, 550),

in the central hub (300), initiating a deposit of the amount of money in the electronic payment cheque into the account of the second user by initialising a verification of the second signature at the banking institution (550) of the second user and a verification of the first signature at the banking institution (500) of the first user.

20. A method according to claim 19, wherein the second private key is generated on the second SIM card (102a).

21. A method according to claim 19 or 20, wherein the signed received payment cheque is transmitted as a Short Message by means of the Short Message Service system over the GSM system.

22. A method according to any of the claims 19 to 21, wherein the signed received electronic payment cheque is transmitted via a message proxy in the central hub (300).

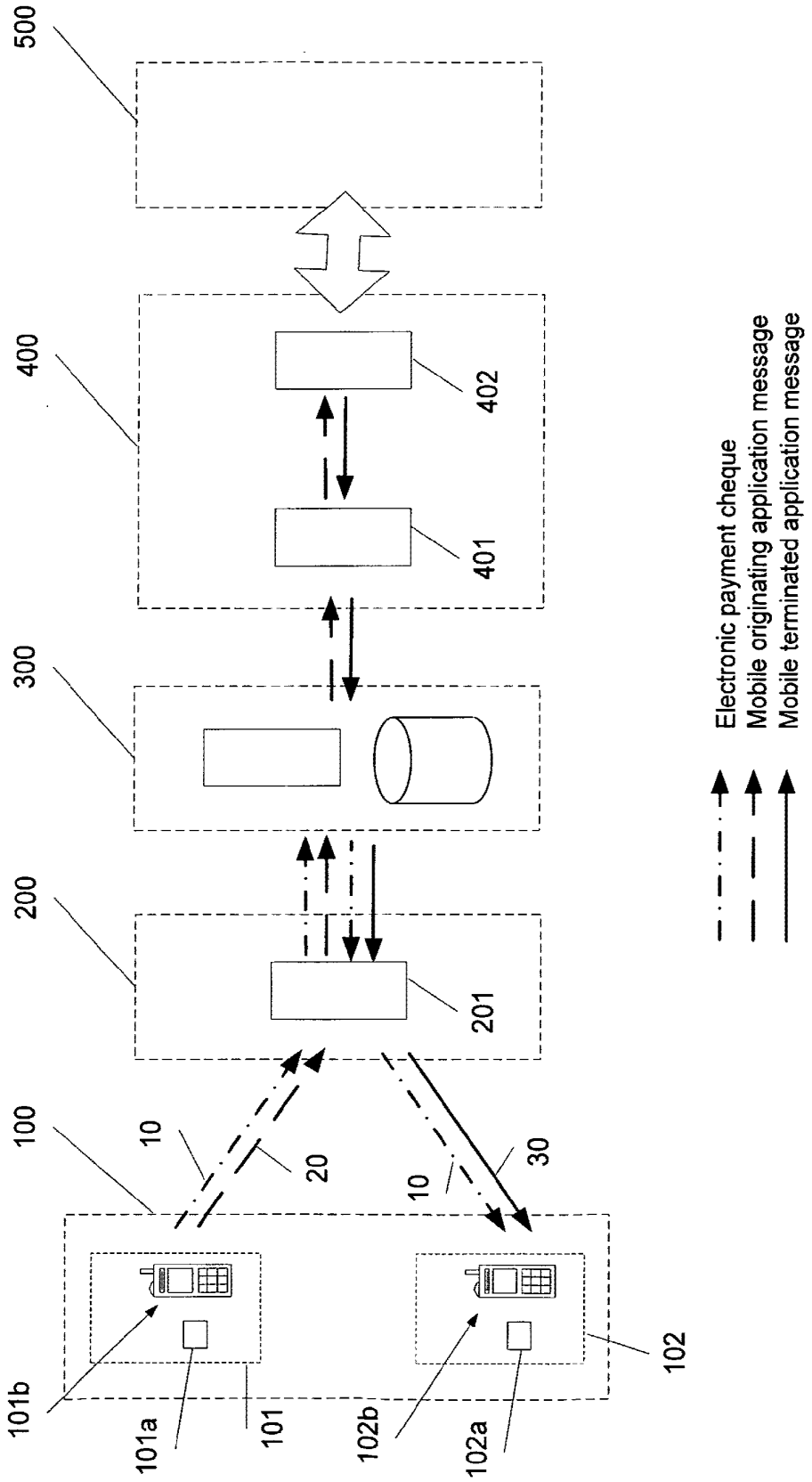

500
400
402
401
300
200
201
100
10
20
10
30
101b
101a
101
102b
102a
102
Electronic payment cheque
Mobile originating application message
Mobile terminated application message

Fig. 1a

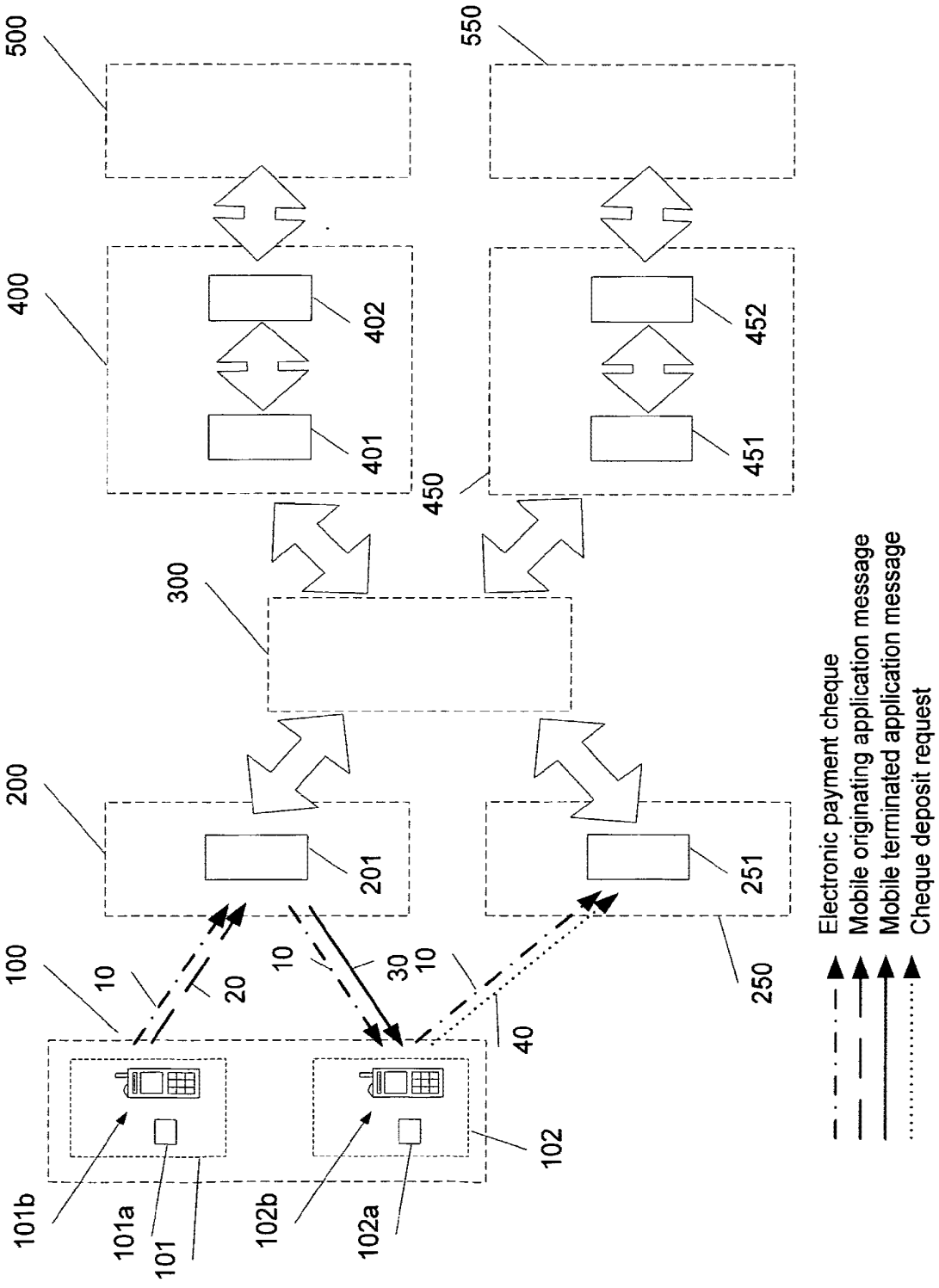

500
550
400
402
452
401
451
450
300
200
201
251
250
100
10
20
10
30
10
40
101b
101a
101
102b
102a
102
Electronic payment cheque
Mobile originating application message
Mobile terminated application message
Cheque deposit request

Fig. 1b

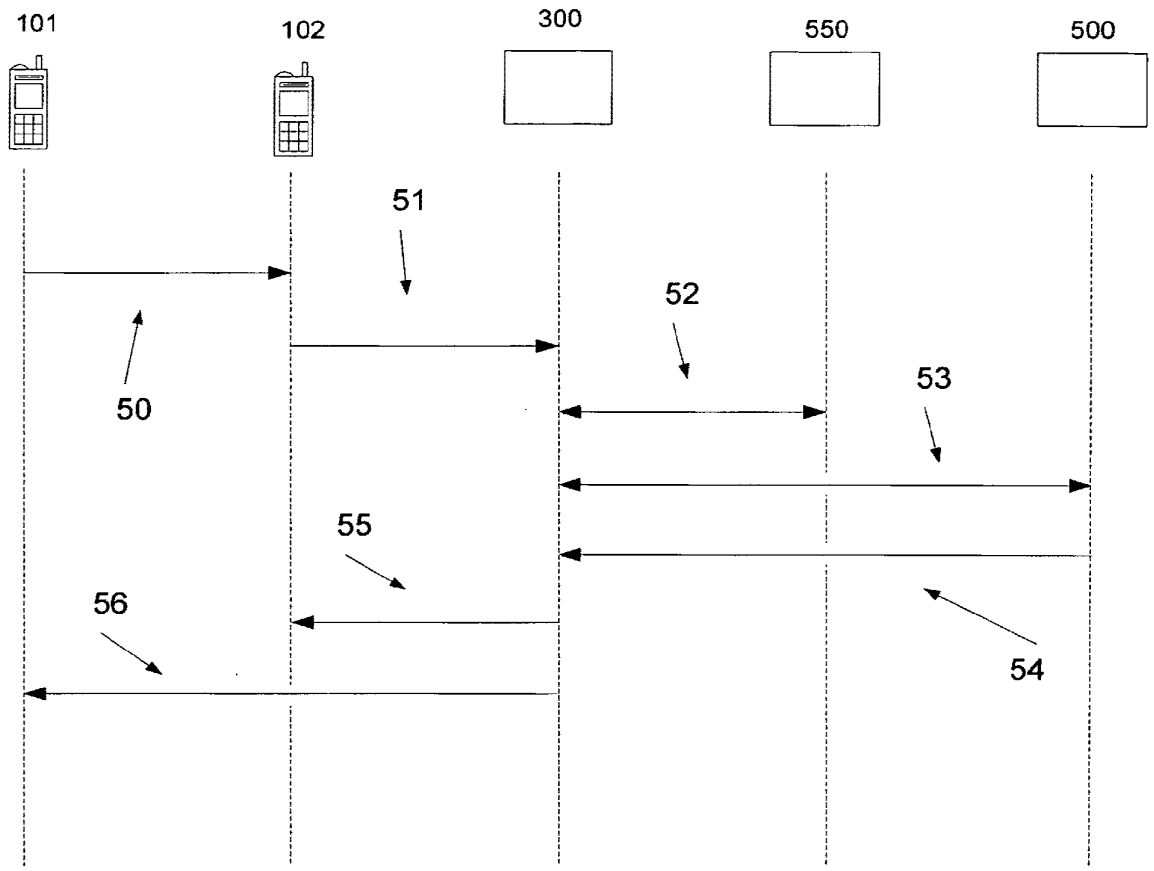


Fig. 2

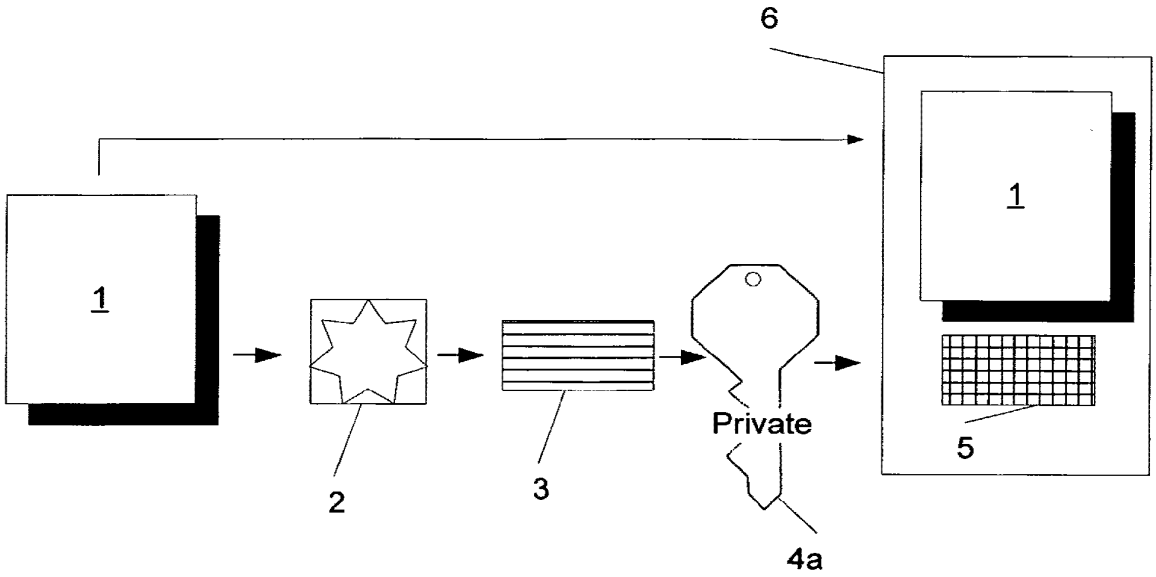


Fig. 3a

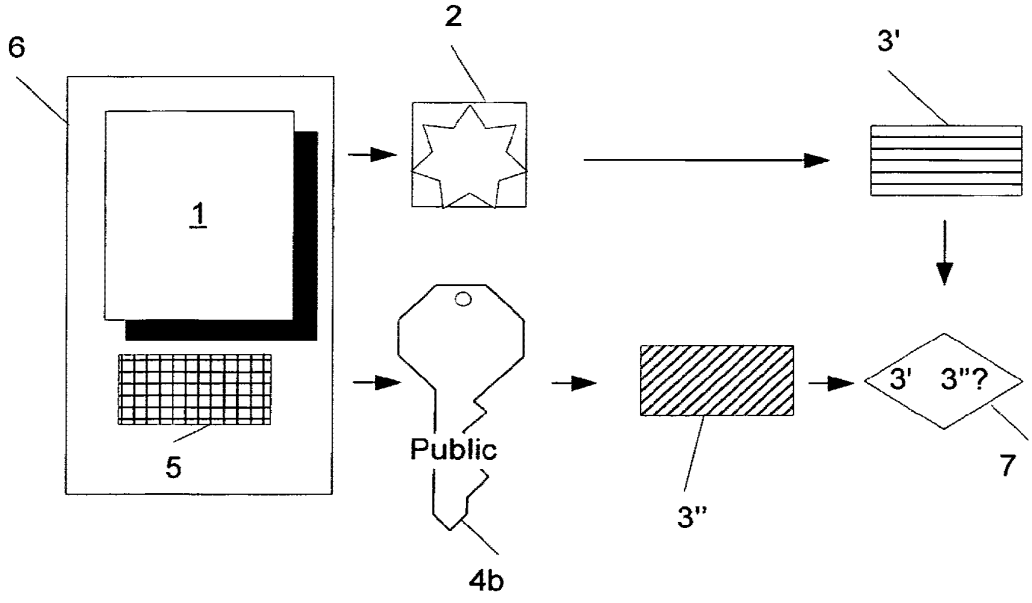


Fig. 3b

INTERNATIONAL SEARCH REPORT

Int onal Application No
PCT/DK 03/00163

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 H04L12/28 G07F19/00

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 H04L G07F

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ, INSPEC

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 677 955 A (ANDERSON MILTON M ET AL) 14 October 1997 (1997-10-14) cited in the application column 3, line 2 -column 6, line 41	1-3,5,6, 8,11-13, 15,16, 19,20
A	EP 0 986 275 A (SWISSCOM AG) 15 March 2000 (2000-03-15) column 3, line 49 -column 5, line 12	1-22
A	US 5 511 121 A (YACOBI YACOV) 23 April 1996 (1996-04-23) column 8, line 40-45 column 9, line 29 -column 10, line 1	1-22

☐ 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	Date of mailing of the international search report
13 May 2003	20/05/2003

Name and mailing address of the ISA	Authorized officer
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	Weinmiller, J

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Inte ›nal Application No
PCT/DK 03/00163

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 5677955	A	14-10-1997	BR	9608448 A	07-12-1999
			CA	2217593 A1	10-10-1996
			EP	0819345 A1	21-01-1998
			JP	11503541 T	26-03-1999
			WO	9631965 A1	10-10-1996
EP 0986275	A	15-03-2000	EP	0986275 A1	15-03-2000
			JP	2000163487 A	16-06-2000
			US	6415156 B1	02-07-2002
US 5511121	A	23-04-1996	CA	2182173 A1	31-08-1995
			EP	0746923 A1	11-12-1996
			JP	9505169 T	20-05-1997
			WO	9523465 A1	31-08-1995

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
2 October 2003 (02.10.2003)

PCT

(10) International Publication Number
WO 03/081519 A2

(51) International Patent Classification[7]: G06K 7/00

(21) International Application Number: PCT/US03/08638

(22) International Filing Date: 19 March 2003 (19.03.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/366,098 19 March 2002 (19.03.2002) US
60/379,964 13 May 2002 (13.05.2002) US

(71) Applicant: CHAMELEON NETWORK INC. [US/US]; Suite 1400, 950 Winter Street, Waltham, MA 02451 (US).

(72) Inventors: THOMAS, Joseph, A.; 34 Warren Street, Westborough, MA 01581 (US). JESSEN, Karlin, B.; 97 Pleasant Street, Reading, MA 01867 (US). BURGER, Todd, O.; 386 Lincoln Street, Lexington, MA 02421 (US). HASSOL, Joshua, L.; 28 Wachusett Drive, Lexington, MA 02421 (US).

(74) Agent: PRITZKER, Randy, J.; Wolf, Greenfield & Sacks, P.C., 600 Atlantic Avenue, Boston, MA 02210 (US).

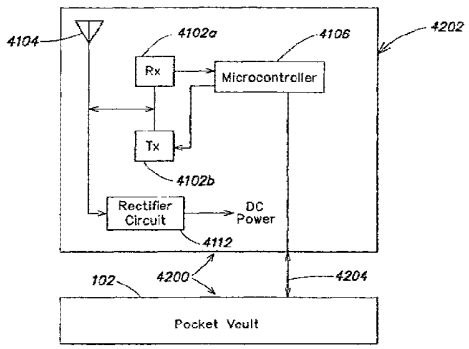
(81) Designated State *(national)*: CA.

(84) Designated States *(regional)*: European patent (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).

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

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

(54) Title: PORTABLE ELECTRONIC AUTHORIZATION SYSTEM AND METHOD



(57) Abstract: In one embodiment, an apparatus comprises a user authenticator and a transponder. The transponder is permitted to emit a wireless signal representing information stored in the apparatus in response to a wireless interrogation signal after the user authenticator has authenticated the identity of the user. In another embodiment, an apparatus comprises, a memory, a user input, and a transponder. The memory stores at least first and second distinct codes. The user input permits a user to select any one of the at least first and second codes for transmission in response to a wireless interrogation signal. The transponder emits a wireless signal representing the selected one of the at least first and second code sin response to an interrogation signal. In yet another embodiment, a token that may be used to engage in a transaction at a point of sale comprises a substrate, a rewritable memory, and a reconfigurable display. The rewriteable memory is supported by the substrate and can be selectively configured to store information on the token that identifies an account that is to be used to engage in the transaction at the point of sale. The substrate and memory are configured and arranged such that the substrate can be selectively interfaced with an apparatus at the point of sale to permit the apparatus to read the contents of the memory. The reconfigurable display is also supported by the substrate and displays at least some of the information that is stored in the rewritable memory.

WO 03/081519 A2

PORTABLE ELECTRONIC AUTHORIZATION SYSTEM AND METHOD

RELATED APPLICATIONS

This application is a Continuation-in-Part (CIP) of Application Serial No. 09/968,628, filed October 1, 2001, and now pending, which is a CIP of U.S. Application Serial No. 09/675,438, filed September 28, 2000, and now pending, which claims the benefit of each of: (1) Application Serial No. 60/156,356, filed September 28, 1999; (2) Application Serial No. 60/167,050, filed November 23, 1999; (3) Application Serial No. 60/184,425, filed February 23, 2000; and (4) Application Serial No. 60/217,542, filed July 12, 2000. This application also claims the benefit of each of (1) Application Serial No. 60/366,098, filed March 19, 2002, and (2) Application Serial No. 60/379,964, filed May 13, 2002.

FIELD OF THE INVENTION

The present inventions are directed to novel systems and methods for engaging in transactions involving financial and/or non-financial media.

BACKGROUND OF THE INVENTION

People often times carry wallets with them when they engage in their day to day activities. A typical wallet is made of leather or other suitable material, and is generally a foldable structure that readily fits into a pocket or purse. A wallet typically includes a number of pockets, pouches, or the like for storing items such as a driver's license, a social security card, identification cards, credit cards, debit cards, membership cards, commuter passes, access tools, business cards, cash, coupons, event tickets, transportation tickets, frequent customer cards (e.g., a frequent flier card), medical information cards, receipts, photographs, etc.

Wallets are frequently stolen, lost, or misplaced. When any of these events occurs, not only must the wallet itself be replaced, but all of the contents of the wallet must be replaced as well. As anyone who has lost a wallet can testify, replacing the contents of a wallet can be cumbersome and expensive. In addition, if a wallet is stolen or if a lost wallet falls into the wrong hands, the contents of the wallet may be used to engage in unauthorized activities which financially detriment the wallet owner, as well as

any banks, credit issuers, and/or other institutions that issued financial media to the wallet owner.

While the wallet owner is generally able to "cancel" financial media in such situations by contacting the respective financial media issuers, often times this is done too late, i.e., after one or more media have been exploited by the unauthorized user. In some cases, the wallet owner may not recall all of the contents of the now stolen wallet, and so may fail to report theft of one or more items. Further, in addition to any cash contained in a lost or stolen wallet, many media issued by non-financial media issuers have a significant cash value, e.g., transportation tickets, event tickets, commuter passes, and the like, and therefore represent an immediate (and often times unrecoverable) financial loss to the wallet owner. Moreover, the misappropriation of media issued by non-financial media issuers that contain personal information, e.g., a drivers license, social security card, identification card, etc., present the opportunity for an unauthorized possessor of a wallet to engage in the practice known as "identity theft," whereby the possessor may assume the identity of the wallet owner for various fraudulent purposes, e.g., using the assumed identity to obtain and exploit one or more new financial media.

Another device commonly used to engage in or authorize transactions is a radio frequency identification (RFID) tag. In an RFID system, an "interrogator" broadcasts a radio frequency (RF) signal which, if received by an RFID tag, causes the RFID tag to return an RF signal to the interrogator that includes information from the tag that may be used to authorize a transaction. Situations in which such tags have been employed include, e.g., automated toll booths and gasoline service stations. RFID tags may be made relatively small in size and therefore may be kept virtually anywhere, e.g., on a keychain or clipped to an automobile visor. Unfortunately, while this aspect of these devices make them convenient, it also makes them highly susceptible to loss or theft. Whenever an RFID tag falls into the wrong hands, there is potential for it to be misused for a long period of time before it is discovered to be missing and some action is take to disable the account associated with it so that it can no longer be used to authorize transactions.

SUMMARY OF THE INVENTION

According to one aspect of the present invention, an apparatus comprises a user authenticator and a transponder. The transponder is permitted to emit a wireless signal

representing information stored in the apparatus in response to a wireless interrogation signal after the user authenticator has authenticated the identity of the user.

According to another aspect, an apparatus comprises, a memory, a user input, and a transponder. The memory stores at least first and second distinct codes. The user input permits a user to select any one of the at least first and second codes for transmission in response to a wireless interrogation signal. The transponder emits a wireless signal representing the selected one of the at least first and second codes in response to an interrogation signal.

According to yet another aspect, a token that may be used to engage in a transaction at a point of sale comprises a substrate, a rewritable memory, and a reconfigurable display. The rewriteable memory is supported by the substrate and can be selectively configured to store information on the token that identifies an account that is to be used to engage in the transaction at the point of sale. The substrate and memory are configured and arranged such that the substrate can be selectively interfaced with an apparatus at the point of sale to permit the apparatus to read the contents of the memory. The reconfigurable display is also supported by the substrate and displays at least some of the information that is stored in the rewritable memory.

According to another aspect, a method for using an apparatus comprises steps of using the apparatus to authenticate an identity of a user of the apparatus, and after the apparatus has authenticated the identity of the user, enabling a transponder of the apparatus to emit a wireless signal representing information stored in the apparatus in response to a wireless interrogation signal.

According to another aspect, a method for using an apparatus comprises steps of manipulating a user input on the apparatus to select one of at least first and second codes stored in memory, and permitting a transponder of the apparatus to emit a wireless signal representing the selected one of the at least first and second codes in response to a wireless interrogation signal.

According to yet another aspect, a method for configuring a token to be used to engage in a transaction at a point of sale involves a step of configuring a rewritable memory of the token to store information that identifies an account that may be used to engage in the transaction at the point of sale. The memory is configured and arranged on the token such that the token can be selectively interfaced with an apparatus at the point of sale to permit the apparatus to read the contents of the memory. The method further

involves a step of configuring a display on the token to display at least some of the information that is stored in the rewritable memory.

According to another aspect, a method is disclosed for enabling a software module on a computer operated by a user to access restricted information on a server. With an electronic device distinct from the computer, an identity of the user is authenticated to determine that the user is permitted to access the restricted information on the server. In response to the electronic device authenticating the identity of the user, the software module on the computer is permitted to access the restricted information on the server.

According to another aspect, a method is disclosed for altering settings on a computer to correspond to settings on an electronic device distinct from the computer. With the electronic device, an identity of a user is authenticated to determine that the user is authorized to use the electronic device. In response to authenticating the identity of the user, the settings on the computer are altered to correspond to settings on the electronic device.

According to another aspect, a system for enabling a software module on a computer operated by a user to access restricted information on a server includes an electronic device which includes a user-authenticator to authenticate an identity of the user to determine that the user is permitted to access the restricted information on the server. The system further comprises means for, in response to the electronic device authenticating the identity of the user operating the computer, enabling the software module on the computer to access the restricted information on the server.

According to yet another aspect, a system for altering settings on a computer to correspond to settings on an electronic device distinct from the computer comprises a user authenticator included in the electronic device to authenticate an identity of a user to determine that the user is authorized to use the electronic device. The system further comprises means for, in response to authenticating the identity of the user, altering the settings on the computer to correspond to settings on the electronic device.

According to another aspect, an apparatus includes a housing; a user authenticator, supported by the housing, that authenticates an identity of a user; at least one memory, supported by the housing, that stores transaction information for at least first and second media; and at least one output, supported by the housing, that releases at

least a portion of the transaction information to a point-of-sale (POS) terminal after the user authenticator has authenticated the identity of the user.

According to another aspect, a method involves steps of: (a) storing transaction information for at least first and second media in a memory of a device (b) using the device to authenticate an identity of a user; and (c) after authenticating the identity of the user with the device, transferring at least a portion of the transaction information from the device to a point-of-sale (POS) terminal.

According to another aspect, an apparatus includes: a housing; at least one memory, supported by the housing, that stores transaction information for at least one media; a user authenticator, supported by the housing, that authenticates an identity of a user of the apparatus; and at least one output, supported by the housing, that, after the user authenticator has authenticated the identity of the user, releases an embedded identification code of the apparatus from the housing that enables a device receiving the embedded identification ID code to authenticate the identity of the apparatus.

According to another aspect, a method involves steps of: storing transaction information for at least one media in a memory of a first device; using the first device to authenticate an identity of a user; and after authenticating the identity of the user with the first device, releasing an embedded identification code of the apparatus from the housing that enables a second device receiving the embedded identification code to authenticate the identity of the first device.

According to another aspect, an apparatus includes: at least one memory that stores transaction information for at least first and second media; at least one input that enables a user to select one of the at least first and second media; a display that provides a visual indication to the user regarding which of the at least first and second media has been selected with the at least one input; and at least one output that selectively releases at least a portion of the transaction information to a point-of-sale (POS) terminal.

According to another aspect, a method involves steps of: storing transaction information for at least first and second media in a memory of a device; receiving as input a user's selection of one of the at least first and second media; displaying a visual indication to the user regarding which of the at least first and second media has been selected; and transferring at least a portion of the transaction information from the device to a point-of-sale (POS) terminal.

According to another aspect, an apparatus includes: at least one memory that stores transaction information for at least one financial media and at least one non-financial media; and at least one output that selectively releases at least a portion of the transaction information to a point-of-sale (POS) terminal.

According to another aspect, a method involves steps of: storing transaction information for at least one financial media and at least one non-financial media in a memory of a device; and transferring at least a portion of the transaction information from the device to a point-of-sale (POS) terminal.

According to another aspect, a system includes: a housing; at least one memory, supported by the housing, that stores transaction information for at least one media; a device releasably attached to the housing; and configuring means, supported by the housing, for selectively configuring the device to hold the transaction information so that the device may be used to engage in a transaction involving the at least one media.

According to another aspect, a method involves steps of: (a) storing transaction information for at least one media in a memory of a first device, the first device having a second device releasably attached thereto; (b) while the second device is attached to the first device, configuring the second device to hold the transaction information for the at least one media based on the contents of the memory; (c) detaching the second device from the first device; and (d) using the second device to engage in a transaction involving the at least one media.

According to another aspect, a system includes: a first device including a user authenticator that authenticates an identity of a user; and a second device releasably attached to the first device, wherein the second device holds transaction information for at least one media so that the second device may be used to engage in a transaction involving the at least one media, and wherein the second device is detached from the first device after the user authenticator has authenticated the identity of the user.

According to another aspect, a method involves steps of: with a first device, authenticating an identity of a user; and after authenticating the identity of a user with the first device, detaching a second device from the first device, the second device holding transaction information for at least one media so that the second device may be used to engage in a transaction involving the at least one media.

According to another aspect, a system includes: a first device; a second device that has the first device releasably attached thereto, the second device including means for selectively configuring the first device to hold transaction information for a first media but not for a second media so that the first device may be used to engage in a transaction involving the first media but not the second media, and the second device further including means for selectively configuring the first device to hold transaction information for the second media but not for the first media so that the first device may be used to engage in a transaction involving the second media but not the first media.

According to another aspect, a method involves steps of: selectively configuring a device to hold transaction information for a first media but not for a second media so that the device may be used to engage in a transaction involving the first media but not the second media; and selectively configuring the device to hold transaction information for the second media but not the first media so that the device may be used to engage in a transaction involving the second media but not the first media.

According to another aspect, a system includes: at least one memory that stores first transaction information for a first media; at least one output that selectively releases at least a portion of the first transaction information to a point-of-sale (POS) terminal; and means for enabling a person to whom the first media is issued to selectively add second transaction information for a second media to the memory.

According to another aspect, a method involves steps of: storing first transaction information for a first media in a memory of a device; releasing at least a portion of the first transaction information to a point-of-sale (POS) terminal; and in response to a request by the person to whom the first transaction information is issued, adding second transaction information for a second media to the memory.

According to another aspect, a system includes: at least one memory that stores first transaction information for a first media and second transaction information for a second media; at least one output that selectively releases at least a portion of the first transaction information to a point-of-sale (POS) terminal; and means for enabling a person to whom the first media is issued to selectively remove at least a portion of the second transaction information from the memory.

According to another aspect, a method involves steps of: storing first transaction information for a first media and second transaction information for a second media in a memory of a device; releasing at least a portion of the first transaction information to a

point-of-sale (POS) terminal; and, in response to a request by the person to whom the second media is issued, removing at least a portion of the second transaction information from the memory.

According to another aspect, a system includes: at least one memory that stores transaction information for at least one media; at least one output that selectively releases at least a portion of the transaction information to a point-of-sale (POS) terminal; and means for enabling at least one functional characteristic of the at least one media to be altered by altering the contents of the least one memory.

According to another aspect, a method involves: storing transaction information for at least one media in a memory of a device; releasing at least a portion of the transaction information to a point-of-sale (POS) terminal; and altering at least one functional characteristic of the at least one media by altering the contents of the least one memory.

According to another aspect, an apparatus includes: a housing; a user authenticator, supported by the housing, that authenticates an identity of a user; at least one memory that, supported by the housing, stores first transaction information for a first media and second transaction information for a second media; and at least one output, supported by the housing, that releases the first transaction information only after the user authenticator has authenticated the identity of the user, and that releases the second information without requiring the user authenticator to have authenticated the identity of the user.

According to another aspect, a method involves steps of: storing first transaction information for a first media and second transaction information for a second media in at least one memory of a device; using the device to authenticate an identity of a user; releasing the first transaction information only after the identity of the user has been authenticated; and releasing the second transaction information without requiring the identity of the user to be authenticated.

According to another aspect, a system includes: a first device; and a second device having the first device releasably attached thereto such that, when the first device is attached to the second device, the second device causes the first device to generate a machine-readable code for only a predetermined, finite period of time after the first device is detached from the second device.

According to another aspect, a method involves a step of generating a machine-readable code on a device for only a predetermined, finite period of time.

According to another aspect, an apparatus includes: a portable substrate; a power supply supported by the substrate; and at least one controller supported by the substrate and powered by the power supply, the at least one controller being configured to generate a simulated magnetic stripe on the substrate.

According to another aspect, an method involves a step of generating a simulated magnetic stripe on a portable device.

According to another aspect, a system includes: at least one memory that stores transaction information for at least one media; a user authenticator that authenticates an identity of the user; and a display that provides a visual indication to the user regarding the at least one media, the visual indication being displayed for only a predetermined, finite period of time after the user authenticator has authenticated the identity of the user.

According to another aspect, a method involves steps of: authenticating an identity of a user; and displaying a visual indication to the user regarding the at least one media for only a predetermined, finite period of time after authenticating the identity of the user.

According to another aspect, a system includes a portable device that can be used to engage in point-of-sale (POS) transactions; and a device remote from the portable device, that can disable an ability of the portable device to engage in POS transactions.

According to another aspect, a method involves steps of: providing a portable device that can be used to engage in point-of-sale transactions; and at a location remote from the portable device, disabling an ability of the portable device to engage in POS transactions.

According to another aspect, a method involves steps of: storing transaction authorization information for at least two media in a first memory of a first device; and storing the transaction authorization information for the at least two media in a second memory, which is disposed at a location remote from the first device.

According to another aspect, a system includes: a first device; and a second device having the first device releasably attached thereto such that, when the first device is attached to the second device, the second device can cause the first device to generate a machine-readable code after the first device is detached from the second device, the second device including at least one controller configured so as to be capable of causing

the first device to generate the machine-readable code only for a finite, predetermined period of time.

According to another aspect, a method involves a step of configuring a first device such that the first device is capable, for only a predetermined, finite period of time, of generating a machine-readable code on a second device.

According to another aspect, a method involves steps of: receiving information at a first device that has been transmitted over an electronic communication link; and after receiving the information at the first device, using a media at the first device to access a quantity of credit or cash reserves that could not be accessed prior to the first device receiving the information.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram illustrating an example of a network system in which a portable electronic authorization device (also referred to herein as a "Pocket Vault") may be employed according to one embodiment of the invention;

Fig. 2 is a block diagram showing an illustrative embodiment of the Pocket Vault shown in Fig. 1;

Fig. 3 is a block diagram showing an illustrative embodiment of one of the interface stations shown in Fig. 1;

Fig. 4 is a block diagram showing an illustrative embodiment of the network server(s) shown in Fig. 1;

Fig. 5 is a diagram showing an example of how the memory of the Pocket Vault shown in Fig. 2 may be configured in accordance with one embodiment of the invention;

Fig. 6 is a block diagram showing an illustrative embodiment of the token (e.g., a card) associated with the Pocket Vault shown in Fig. 2;

Fig. 7 is a flow diagram illustrating a primary routine that may be executed by the controller of the Pocket Vault shown in Fig. 2;

Fig. 8 is a flow diagram illustrating an example implementation of the PROCESS POCKET VAULT VALIDATION routine shown in Fig. 7;

Fig. 9 is a flow diagram illustrating an example implementation of the UNAUTHORIZED HOLDER routine shown in Fig. 7;

Fig. 10 is a flow diagram illustrating an example implementation of the AUTHORIZED HOLDER routine shown in Fig. 7;

Fig. 11 is a flow diagram illustrating an example implementation of the PROCESS CARD TRANSACTION routine shown in Fig. 10;

Fig. 12 is a flow diagram illustrating an example implementation of the VERIFY CARD RETURN routine shown in Fig. 7;

Fig. 13 is a flow diagram illustrating an example implementation of a primary routine that may be executed by the controller of the pocket vault interface unit shown in Fig. 3;

Fig. 14 is a flow diagram illustrating an example implementation of a primary routine that may be executed by the controller of the interface station computer shown in Fig. 3;

Fig. 15 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO VALIDATE POCKET VAULT routine shown in Fig. 14;

Fig. 16 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO UPDATE INFO ON POCKET VAULT routine shown in Fig. 14;

Fig. 17 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO AUTHORIZE TRANSACTION routine in Fig. 14;

Fig. 18 is a flow diagram illustrating an example implementation of the PROCESS UNSUCCESSFUL OPERATOR AUTHENTICATION routine shown in Fig. 14;

Fig. 19 is a flow diagram illustrating an example implementation of a primary routine that may be executed by the controller(s) of the network server(s) shown in Fig. 4;

Fig. 20 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO REGISTER NEW POCKET VAULT HOLDER routine shown in Fig. 19;

Fig. 21 is a flow diagram illustrating an example implementation of the PROCESS REQUEST BY MEDIA ISSUER/ADVERTISER TO UPDATE NETWORK SERVER routine shown in Fig. 19;

Fig. 22 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO UPDATE INFO ON POCKET VAULT routine shown in Fig. 19;

Fig. 23 is a flow diagram illustrating an example implementation of the PROCESS REQUEST FROM HOLDER TO LOAD NEW FILE ONTO NETWORK SERVER routine shown in Fig. 19;

Fig. 24 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO AUTHORIZE TRANSACTION routine shown in Fig. 19;

Fig. 25 is a flow diagram illustrating an example implementation of the AUTHORIZED POCKET VAULT USE? routine shown in each of Figs. 20, 22, and 24; and

Figs 26a-26p are illustrations of the portable electronic authorization device, as well as the token (e.g., a card) associated therewith, as these items may appear when in use;

Fig. 27 is a block diagram illustrating several additional features that may optionally be added to a network system such as that shown in Fig. 1 so as to enhance the functionality of the network;

Fig 28 is a block diagram illustrating example components that may optionally be added to software executing on a controller of the Pocket Vault, such as the software described in connection with Figs. 7-12, so as to enhance the functionality of the Pocket Vault in a network environment;

Fig 29 is a data flow diagram illustrating an example of how data may flow between the Pocket Vault and a user interface of an interface station computer to which the Pocket Vault is interfaced/docked;

Fig. 30 is a flow diagram illustrating an example of a primary routine that may be executed by a website on the network server(s) shown in Fig. 27, which website may be accessed, for example, by a browser executing on the interface station computer shown in Fig. 27;

Fig. 31 is a flow diagram illustrating an example implementation of the INSTALL DRIVER(S) routine shown in Fig. 30;

Fig. 32 is a flow diagram illustrating an example implementation of the NEW POCKET VAULT HOLDER routine shown in Fig. 30;

Fig. 33 is a flow diagram illustrating an example implementation of the EXISTING POCKET VAULT HOLDER routine shown in Fig. 30;

Fig. 34 is a flow diagram illustrating an example implementation of the CARD LOADING routine shown in Fig. 33;

Fig. 35 is a flow diagram illustrating an example implementation of the SYNCHRONIZATION routine shown in Fig. 33;

Fig. 36 is a flow diagram illustrating an example implementation of the RECOVERY routine shown in Fig. 33;

Fig. 37 is a flow diagram illustrating an example implementation of the IDENTITY PORTING SELECTION routine shown in Fig. 33;

Fig. 38 is a flow diagram illustrating an example implementation of the BACKUP routine shown in Fig. 33;

Fig. 39 is a flow diagram illustrating an example implementation of the SET PREFERENCES routine shown in Fig. 33;

Fig. 40 is a flow diagram illustrating an example implementation of the RFID TAG LOADING routine shown in Fig. 33;

Fig. 41 is a block diagram showing a prior art RFID tag; and

Fig. 42 is a block diagram showing an example embodiment of an RFID system in which a Pocket Vault such as that shown in Fig. 2 is used to selectively provide data to an RFID tag.

DETAILED DESCRIPTION

Disclosed herein is a new method and system for producing, distributing, storing, and using the typical contents of a person's wallet, as well as the multiple, separate transaction authorization devices, e.g., RFID tags, owned by the person. Essentially, the system may enable individuals to replace nearly all of the paper and plastic contents of their wallets and all of their other transaction authorization implements with a single, hand-held portable electronic authorization device. The system may include the portable electronic authorization devices, removable morphing tokens or cards associated with such devices, associated computer peripherals, software and certain network capabilities. As a whole, the system may eliminate virtually all of the distribution costs and security concerns associated with paper and plastic media.

Because the device may incorporate many different media that are commonly stored in a person's wallet or elsewhere, possibly including both financial and non-financial media, it is much more than a simple point-of-sale (POS) device. Therefore, the device may be more appropriately referred to as a multi-purpose, "point-of-transaction" device. In any situation of presentment, whether for purposes such as

building security, demonstrating membership or using credit or debit capacity, the system is designed to perform tasks more safely, securely and with greater ease than is possible with prior art systems. Further, while certain computer technologies are involved, the preferred embodiment is such that some people may barely recognize it as a computer, seeing instead a more comfortable to carry, easier-to-use, safer and more securely packaged means of transporting typical wallet contents and other items.

The system's business model may comprise an independent organization acting as a media-neutral, multi-service provider of other issuers' various financial and non-financial media, that also may enable individuals and retailers to add or create their own secure (and where appropriate, non-secure media) using a device with a self-contained set of authentication security features, which may even be password-free. This device may operate over existing financial transaction networks, while also having links to a highly secure network system for certain functionality. The self-contained authentication functionality of the device itself ensures privacy, while providing sufficient accountability/traceability to satisfy law enforcement concerns.

A network system 100 configured according to one illustrative embodiment of the invention is shown in Fig. 1. As shown, the network system 100 may include a portable electronic authorization device 102 (alternatively referred to herein as a "Pocket Vault") and an associated token 102a (alternatively referred to herein as a "Chameleon Card"). Each person desiring to use the network system 100 may possess his or her own the Pocket Vault 102 and associated token 102a. Some individuals may choose to own multiple Pocket Vaults or Chameleon Cards. The system and software therefore may accommodate the use of multiple Pocket Vaults and multiple Chameleon Cards by one individual.

Referring to Fig. 1, in addition to the Pocket Vault 102, the network system 100 may include one or more network servers 114 to which various other network components are coupled. Although multiple, load-sharing network servers 114 may be employed in a typical application, the network server(s) 114 will hereinafter, for convenience, occasionally be referred to as a single network server 114. Coupled to the network server 114 are: several different types of interface stations 104 (i.e., a validation interface station 104a, a personal interface station 104b, and a commercial interface station 104c), one or more commercial card readers 106, one or more commercial bar code readers 107, one or more RFID interrogators 116, and several computers 108, 110,

and 112 operated by one or more advertisers, non-financial media issuers, and financial media issuers, respectively. The structure and functionality of each of the components of the network system 100 in accordance with illustrative embodiments of the invention are described below.

As shown in Fig. 1, the network server 114 may form the hub of the network system 100, with each of the interface stations 104, the commercial card readers 106, the commercial bar code readers 107, the RFID interrogators 116, and the computers 108, 110, and 112 being coupled thereto. As discussed in more detail below, the network server 114 may therefore serve as: (1) a repository of information for the network, (2) the entity that controls access to the stored information by the other network devices, and (3) a service provider for financial and non-financial media issuers, advertisers, as well as Pocket Vault holders.

Any of a number of techniques may be used to interconnect the various elements of the network system 100, and the invention is not limited to any particular networking technique. In one illustrative embodiment, for example, the network server 114 is coupled to the other elements in the network system 100 via the Internet or similar packet-switched communication system. Alternatively, dedicated or selectively established (e.g., using a dial-up modem) communication channels or time slots thereof may be employed between the respective devices. The connections between most of the network devices may be either hardwired (including fiber optic connections) or wireless (e.g., infrared (IR) or radio frequency (RF) links).

As shown in Fig. 1, the Pocket Vault 102 may be interfaced with any of the interface stations 104a-c so as to permit information to be uploaded from the network server 114 to the Pocket Vault 102, or to be downloaded from the Pocket Vault 102 to the network server 114. In one illustrative embodiment, each of the interface stations 104 includes a docking mechanism that permits a Pocket Vault 102 to be physically, as well as electronically, interfaced therewith. In such an embodiment, once the Pocket Vault 102 is physically "docked" with an interface station 104, the Pocket Vault 102 may communicate with the interface station 104 using any now known or later discovered technique. For example, physical contact may be made between respective electrodes or plugs, a line of sight (e.g., infrared) wireless link may be established, or any other interfacing technique may be employed.

The Pocket Vault 102 may additionally or alternatively be configured such that it need not be physically docked with or even in the same room as the interface station 104, as a wireless network such as Bluetooth may be employed to permit communication between devices on the network system 100. In fact, in some embodiments wherein appropriate networking capabilities are provided, each Pocket Vault 102 may communicate directly with the network server 114, without the interface stations 104a-c facilitating communication therebetween. In addition, in some embodiments, Pocket Vaults 102 may communicate directly with one another. In such embodiments, such inter-device communication may permit value to be exchanged directly between Pocket Vaults 102.

The personal docking station 104b may allow setting or changing of user preferences, recording of miscellaneous information by the Pocket Vault holder, replenishment or deletion of information regarding particular media, and may also permit additional media (e.g., a library card) to be added to the device. The Pocket Vault holder may, for example, directly add non-value-based media (e.g., a membership number for the local Historical Society) and notes to the Pocket Vault 102. In one embodiment, value-based and certain identification media (a driver's license, passport, building security ID, etc.) may be added or reinstated only through a secure connection to the network server 114 (as described below), in response to an update request from the Pocket Vault holder. In addition, the personal interface station may provide a mechanism to download transaction activity involving the Pocket Vault 102 into an individual's home computer. There are many users of home finance software. These applications can be relatively "data hungry," and commonly require users to download checking and debit card data from their banks (or key it in manually) and to key in the details of credit card and cash purchases. All of this keying and internet file downloading from third parties may be replaced by a simple docking procedure, i.e., when the Pocket Vault 102 is interfaced with the personal docking station 102b.

As shown in Fig. 1, and as described below in more detail, the Pocket Vault 102 may be equipped to generate the token 102a such that the token 102a has transactional information regarding a media (e.g., an actual or simulated magnetic stripe or a bar code) produced thereon. In such an embodiment, after the token 102a has been generated, the token 102a may be used by the Pocket Vault holder to engage in a transaction wherein an entity swipes the magnetic stripe portion of the token 102a through a card reader 106 or

scans the bar code on the token 102a using a bar code reader 107. Additionally or alternatively, the token 102a may include a suitable Smartcard interface so that it may be used with Smartcard compatible devices.

Because the token 102a may be caused to take on a different personality each time it is released from the Pocket Vault 102, a plurality of media may be stored electronically in memory of the Pocket Vault 102, and the token 102a may, upon request, be generated to take on the personality selected by the Pocket Vault holder. The respective media stored on the Pocket Vault 102 may be issued by different and unrelated media issuers. As used herein, two media issuers are "unrelated" if there exists no legal relationship between them.

The token 102a may also have display capacity. Such a display may, for example, indicate the media personality the token 102a has taken on. In addition, for security purposes, the account number of the media, and perhaps other information, for example, the three digit security code typically found on credit cards, may be shown on the display of the token 102a after it is ejected from the Pocket Vault. The display of this information may help prevent fraudulent uses of the token 102a because the entity accepting it would be able to verify that the displayed information matched that read by the device used to read the token 102a, e.g., a magnetic card reader.

In some embodiments, value may be exchanged between two Pocket Vaults 102 when one the Pocket Vault 102 generates a token 102a having a value-based or value-linked media stored thereon, and the token 102a so generated is passed to the other the Pocket Vault 102, which then may then access the media and extract value therefrom or add value thereto. As mentioned above, this sort of value exchange may also be accomplished directly between two Pocket Vaults 102 over a wireless network, such as Bluetooth.

As discussed in more detail below, in addition to or in lieu of the token 102a, the Pocket Vault 102 may also generate a bar code for a selected media on the Pocket Vault's display (not shown in Fig. 1), and the bar code reader 107 may be used to scan the displayed bar code to process a transaction. Further, a transaction may be processed via a commercial interface station 104c either by use of a docking terminal or via a wireless network scheme such a Bluetooth. In one embodiment, some commercial interface stations 104c may comprise an interface station linked to a standard commercial

card reader 106 or commercial bar code reader 107, with the card reader 106 or bar code reader 107 being modified to accept input from the station.

Moreover, as is also discussed in more detail below, the Pocket Vault 102 may be configured or programmed to function as an RFID tag that can be used only by an authorized user of the Pocket Vault 102. For example, in response to an interrogation signal from the RFID interrogator 116 (e.g., an interrogator of an automated toll booth), the Pocket Vault 102 (if authorized) can return an appropriate RF signal to authorize payment of the required fee for the toll. In some embodiments, the RFID functionality of the Pocket Vault 102 can be altered by the user so that user is permitted to select the personality of the RFID tag that is embodied by the device. The user may, for example, first use the Pocket Vault 102 as an RFID tag to authorize payment of a toll, and later use the same Pocket Vault 102 as an RFID tag to authorize payment at a service station.

To permit the Pocket Vault holder to select from among the various media stored in memory of the Pocket Vault 102, the Pocket Vault 102 may comprise a display (not shown in Fig. 1). By employing either a display having a user-manipulable touch screen or a separate user input device (not shown in Fig. 1), a Pocket Vault holder can effectively flip through the contents of the Pocket Vault 102 to locate and select a desired media (e.g., a credit card, driver's license, library card, frequent flier card, a particular RFID personality, etc.) much like a person can flip through the contents of his or her wallet to do the same.

The use of a display on the Pocket Vault 102 also creates an opportunity for media providers to go from a static presentation of their brand (logo, etc.) to having the option of dynamic branding and messaging. In addition, using the display, the presentment of active marketing at the "moment of buying decision" is possible. Specifically, the logo and message displayed to the Pocket Vault holder may incorporate motion, moving images and messages. To conserve power, moving images may be presented only at certain times, e.g., in response to internal or external events or communications.

In the embodiment of Fig. 1, the computers 108, 110, and 112, together with the network server 114, may represent a secure infrastructure of server databases capable of storing information for purposes of delivering personalized services to holders of Pocket Vaults 102. The network server 114 may also track activity of Pocket Vault holders and compile marketing information based thereupon that may prove useful to media issuers

and/or advertisers. The Pocket Vault holder may have control over the ability of the network server 114 to track activity. The information maintained on the network system 100 may originate with the holders of Pocket Vaults 102 and/or may originate with the other entities having access to the network system 100 (e.g., advertisers and media issuers).

As discussed below in more detail, in some embodiments of the invention, certain uses of the Pocket Vault 102, as well as each of the interface stations 104a-c, may be permitted only by pre-authorized individuals. To this end, a suitable user authentication technique may be employed in connection with each attempted use of any of these devices. One suitable user authentication technique that may be employed is the analysis of a bio-metric feature of the individual attempting use of the device (e.g., a fingerprint scan, retina scan, a speech pattern analysis, keystroke rhythm, etc.), and validating the identity of the individual on that basis. Alternatively or additionally, a personal identification (PIN) code may be entered by the holder to verify the holder's identity. In one illustrative embodiment, authentication information used to validate the holder's identity (e.g., the stored fingerprint and/or PIN code) is stored within the to-be-accessed device, and the validation is performed in its entirety on-board the same device, such that the user-specific authentication information never leaves the device in which it is stored. Thus, using this technique, the likelihood that such information will be intercepted by unauthorized third parties may be reduced significantly.

It should be appreciated that, for some applications, it may be desirable to receive and store authentication information (e.g., fingerprint data) of some or all Pocket Vault holders in the network server 114. Accordingly, in some embodiments, such authentication information may be maintained by the network server 114. This authentication information may be transmitted to the network server 114, for example, when Pocket Vaults 102 are first validated.

As discussed below, great care may be taken to ensure that only authorized individuals are permitted to validate Pocket Vaults 102 by having their authentication information (e.g., their fingerprint data or PIN codes) stored therein. Therefore, after it has been confirmed that the holder's authentication information has been properly stored in the Pocket Vault 102, a trust relationship may be established between the network server 114 and the Pocket Vault 102. This relationship may involve, for example, the registration of a unique encrypted chip ID of the Pocket Vault 102 with the network

server 114 through a secure Internet connection, the distribution of a digital certificate (e.g., a PKI certificate) to the Pocket Vault 102, and the grant of authority to the Pocket Vault 102 to permanently store the Pocket Vault holder's authentication information.

A similar level of care may also be taken to ensure that only authorized individuals are permitted to validate interface stations 104a-c by having their authentication information (e.g., their fingerprint data or PIN codes) stored therein. Therefore, as with the Pocket Vaults 102, after it has been confirmed that each interface station's authorization information has been properly stored in the interface station 104, a trust relationship may be set up between the network server 114 and the interface station 104. This relationship may also involve, for example, the registration of a unique encrypted chip ID of the interface station 104 with the network server 114 through a secure Internet connection, the distribution of a digital certificate to the interface station 104, and the grant authority to the interface station 104 to permanently store the interface station operator's authentication information. While, in some embodiments, the Pocket Vault 102 and/or the interface stations 104 are each permitted to store authentication information for only one individual, it should be appreciated that, in alternative embodiments, the Pocket Vault 102 and/or the interface stations 104 may each store authentication information for more than one individual, thereby permitting multiple people to use them.

Because of the creation of the above-described trust relationships, each Pocket Vault 102 and each interface station 104 may communicate securely with the network server 114, as well as with any other networked devices or sites that require a high level of trust. Also, the existence of these trust relationships enable individual Pocket Vaults 102 to accept other services provided by the network servers 114, such as the backup and recovery of information stored within the Pocket Vaults 102. That is, the network servers 114 can serve as a repository for all of the information stored on every validated Pocket Vault 102 (except the holder's authentication information – which, in some embodiments, is stored only in the Pocket Vault 102). To ensure that the network server 114 stores an accurate version of the contents of each Pocket Vault 102, information may, for example, be uploaded from the network server 114 to a Pocket Vault 102 or downloaded from the Pocket Vault 102 to the network server 114 each time the Pocket Vault 102 is interfaced with any of the interface stations 104a-c. Therefore, if a Pocket Vault 102 is lost or stolen, the Pocket Vault holder need only obtain a new Pocket Vault

102, and the entire contents of the lost Pocket Vault 102 can be uploaded thereto, in a single communication, in a matter of seconds. In addition, in the event that a validated Pocket Vault 102 is lost or stolen, the network server 114 may void the chip ID of that Pocket Vault 102, so that the Pocket Vault 102 cannot be used by a third party, even if the holder validation security (e.g., the bio-metric scanning or PIN entry requirement) is somehow breached. Voiding the chip ID of the Pocket Vault 102 may, for example, prevent the Pocket Vault 102 from assigning any media information to the associated Chameleon Card.

In addition to serving as a repository for Pocket Vault information, the network server 114 may also serve as a repository for information regarding media issuers or advertisers, and may further provide various services to these entities. For example, the network server 114 may facilitate transactions involving media issued by media issuers, and may permit new media to be issued or lost media to be replaced at a fraction of the cost of generating new physical tokens or replacing lost ones. Additionally, the network server 114 may serve as a conduit for advertisers to target particular classes of Pocket Vault holders, and channel information to them. The network server 114 may also function as an advocate for Pocket Vault holders, advertisers, and/or media issuers when it utilizes its portfolio of Pocket Vault holders, media issuers, and/or advertisers to secure privileges. Examples of such advocacy include the ability to secure buying power for Pocket Vault holders as a group or to provide media issuers and advertisers with a highly efficient tool for generating awareness for affinities or causes that fit appropriate holder markets. In sum, the services provided by the network server 114 enable Pocket Vault holders to combine and manage their media data using a single, hand-held device, and enables advertisers and media issuers to understand more about, and more readily reach more of, their customers than ever before.

Fig. 2 shows an example embodiment of the Pocket Vault 102 of Fig. 1. The Pocket Vault 102 may employ components similar to those used in modern personal digital assistants (PDAs) and palm top computers. Examples of such products include PDAs such as the "Palm Pilot" from Palm, Inc. (www.palm.com), and the "Casiopedia" from Casio, Inc. of Dover, New Jersey (www.casio.com). As shown, the Pocket Vault 102 may include a controller 202, as well as a transceiver 204, a user input device 206, a docking interface 208, a read/write memory 210, a write-once memory 212, a power manager 214, an indicator 215, a display 216, a token port 218, and a fingerprint scanner

220, all coupled to the controller 202. In addition, the Pocket Vault 102 may include a hard-wired memory (not shown) to store device serial numbers and key operating system and encryption software components.

Actual views of an example embodiment of the Pocket Vault 102, as well as the token 102a associated therewith, are shown in Figs. 26A-26P. The views of Figs. 26A-P, including the items displayed on the display 216, are discussed in more detail below in connection with the flow diagrams of Figs. 7-12. At this point, however, with reference to Figs. 26A-L and 26O, it may be noted that the Pocket Vault 102 may comprise a housing 2602 in which the components shown in Fig. 2 may be disposed. As illustrated in Figs. 26E and 26F, the housing 2602 may be approximately seventy millimeters wide, approximately one hundred millimeters long, and approximately fifteen millimeters deep. Thus, in the embodiment shown, the housing 2602 has an internal volume of less than 105 cubic centimeters.

Of course, in alternative embodiments, the housing 2602 may be slightly larger or smaller than that shown. For example, in different embodiments, the housing 2602 may have an internal volume of less than five hundred cubic centimeters, or less than four hundred cubic centimeters, or less than three hundred cubic centimeters, or less than two hundred cubic centimeters, or less than one hundred cubic centimeters, or less than any other volume value that falls between one hundred and five hundred centimeters. In one embodiment, the housing 2602 is sized so that the Pocket Vault 102 may readily fit into the rear pocket of a pair of pants. One feature of the illustrative embodiment of the Pocket Vault 102 shown in Fig. 2 which may permit its size to be reduced below that of a standard personal computer is the fact that the embodiment shown lacks a disk drive (either hard or floppy) or any similar memory storage device (e.g., a tape drive) that consumes a significant volume within the housing 2602. It should be appreciated, of course, that alternative embodiments may include such memory devices, and that the invention is not necessarily limited to embodiments that exclude them. In addition to the lack of a disk drive or the like, in some embodiments, the power manager 214 may reduce the power consumption of the active components of the Pocket Vault 102 well below that of a standard personal computer, thereby enabling a very small and light weight battery to be employed, as opposed to the relatively large and heavy batteries typically employed in personal computers.

The housing 2602 may provide a water-resistant or waterproof environment for the components housed thereby. The housing 2602 may further be sealed in a manner suitable to prevent tampering, for example, using a plastic potting compound, and may even be designed such that any attempt to invade the housing 2602 will damage the Pocket Vault 102 such that it may no longer be used. The housing materials of Pocket Vaults 102 may be brightly colored, in addition to traditional black or brown, thereby helping their holders to make a fashion statement and/or permitting them to be readily spotted if misplaced. Deluxe versions may be clad in leather, KevlarTM, GortexTM, aluminum and/or stainless steel. In some embodiments, the housing 2602 may even be woven into garments.

Referring again to Fig. 2, any of a number of devices may be used to implement the controller 202, and the invention is not limited to any particular type of controller. In one illustrative embodiment, for example, the controller 202 comprises a low-power multiprocessor or microcomputer having an on-board SRAM and/or flash memory and a real time clock calendar. One example of a suitable controller is the "Motorola Dragonball" Processor from Motorola, Inc. (www.motorola.com). The controller 202 may include a software-programmable and encryption-protected or hard-wired unique chip ID. In one embodiment, this chip ID is released from the Pocket Vault 102 only after the fingerprint scanner 220 (discussed below) has successfully authenticated the identity of the holder. A signal processor for Bluetooth or another wireless connection may also be employed within or along with the controller 202.

The transceiver 204 may include one or more antennas and may be any type of transceiver (or separate transmitter and receiver) capable of communicating with other devices in the network 100 to enable the functionality described herein. For example, either an RF or an IR transceiver may be employed. Some embodiments may, in fact, include both an IR and an RF transceiver to be used in different applications. For example, an IR transceiver may be employed to interface the Pocket Vault with a "docking station" type interface unit, and a separate RF transceiver may be employed to communicate over a wireless network such as Bluetooth. Multiple transceivers (or transmitter/receiver pairs) of the same type may also be employed, if desired.

As discussed in more detail below in connection with Figs. 41 and 42, the transceiver 204 may, for example, serve as the transmitter and receiver of an RFID transponder used to respond to an interrogation signal from an interrogator 116.

In one illustrative embodiment, the user input device 206 is implemented as part of a touch-screen display used as the display 216 (described below). Additionally or alternatively, the user input device 206 may include dedicated buttons, a keypad, a touch pad, a microphone and speech recognition software, a wand or joystick, or any other suitable implement that permits a person to provide input to the controller 202. The user input device 206 may also be integrated into the fingerprint scanner 220 or into an alternative bio-metric input device. By manipulating the user input device 206, a Pocket Vault holder may select one of a number of media stored in memory of the Pocket Vault 102 for display and/or use in connection with a transaction, and may otherwise control or provide input to software executing on the controller 202. In one embodiment, a keypad is employed as the user input device 206, thereby permitting the holder to input a PIN code as a means of authenticating the holder's identity.

The docking interface 208 may take on any of numerous forms, and the invention is not limited to any particular type of interface device. The docking interface 208 may, for example, include a multi-pin plug adapted to mate with a receptacle disposed on the interface units 104a-c, or vice versa. The docking interface 208 may also comprise one or more implements (e.g., grooves or keys) to ensure that the plug or other docking interface 208 mates correctly with the reciprocal device on an interface unit 104 when the two are physically mated together.

The read/write memory 210 may take on any of a number of forms, and the invention is not limited to any particular type of memory. The memory 210 may, for example, comprise a suitable non-volatile SRAM. Similarly, any suitable memory device that permits a only single write operation to take place may be employed as the write-once memory 212. The memory 210 may have instructions stored therein which, when executed by the controller 202, cause the controller 202 to implement the routines/software described below in connection with Figs. 7-12 and/or Fig. 28. Of course, the memory 210 may also contain a suitable operating system (e.g., Palm OS, Microsoft's Windows CE, Microsoft's Windows for Smartcards, or some similar offering), appropriate device drivers, and other software employed in connection with the controller 202 and/or the peripherals thereof. The memory 210 may also be used to store the various media and personal information retained by the Pocket Vault 102. In one illustrative embodiment, the memory 210 stores a plurality of different media issued by different and unrelated media issuers, including both financial (e.g., a credit or debit

card) and non-financial media (e.g., a drivers license or a library card). Other examples of media or information that may be stored in the memory 210 include: a social security card, identification cards, membership cards, discount cards, commuter passes, toll passes, data for various RFID tags, transit cards, access tools such as hotel keys, business cards, coupons, concert and theatre tickets, transportation tickets, frequent customer cards (e.g., a frequent flier card), medical information cards, receipt information, photographs, etc.

As used herein, "financial media" refers to any media which can, as a matter of course, be used to purchase goods or services, whereas "non-financial media" refers to any media which, while possibly having some value to the Pocket Vault holder, cannot, as a matter of course, be used to purchase goods or services. Examples of financial media include value-linked and value-based media such as debit or credit cards issued by a bank or other financial institution, telephone calling cards, etc. Examples of non-financial media include: library cards, driver's licenses, building access cards, etc. In one embodiment, the memory 210 is large enough to store as many as one hundred compressed graphic image files, and full data sets for as many as one hundred types of media.

In addition, the memory 210 may store status information, where useful, for each type of media. Examples of this sort of status information include: information regarding the value remaining on a pre-paid phone card, information regarding an accumulated number of frequent flier miles, information regarding a total number of cups of coffee that have been purchased at a particular coffee shop (e.g., in connection with a buy-ten-get-one-free special), etc. The portion of the memory 210 devoted to memory storage may be divided into three sections: (1) a high-security section, (2) a medium security section, and (3) a non-secure section. The high security section may be used to store value-based or value-linked media such as debit and credit cards and certain ID information such as driver's licenses, passports, building security passes, etc. The medium security section may be used to store low-value, limited use media that may be accessed, for example, by retailers to keep track of frequent purchase credits or the like. The non-secure section may, for example, be used to store notes, membership ID records, emergency contact information, etc. Access to the information included in the various sections may require security or user authentication procedures commensurate with the indicated security level. For example, an accurate fingerprint scan and an

accurate pin code entry may be required to access the high-security section, only an accurate PIN code entry (even by the retailer) may be required to access the medium-security section, and anyone may be permitted to access the non-secure section.

The power manager 214 may comprise any of numerous devices, and the invention is not limited to any particular type of power supply/management device. The power manager may, for example, employ a flat, rechargeable, lithium battery, and associated regulator and power management software. Alternatively, the battery used may be non-rechargeable and/or coin cell-shaped. Solar powered cells may also be a viable option as at least a supplement to battery power, if not a primary source of power for the Pocket Vault 102. This may be made possible because of the typically modest on-time requirements for a Pocket Vault 102. Power management software may also assist in minimizing the power consumption of the Pocket Vault 102. Such software may, for example, invoke an auto-shutdown feature after a preference-set number of seconds, may control the level of screen back-lighting in response to feedback received from a photo-sensor that registers ambient light, and/or may provide battery charge level warnings to Pocket Vault holders.

The indicator 215 may be any device capable of generating a perceptible indication to the holder such as a bell, chime, buzzer, light, vibration, etc., and the invention is not limited to any particular type of device for accomplishing such a result. In one embodiment, for example, the indicator is a chime generator that generates a "chime" sound that can be heard by the Pocket Vault holder.

Any of a number of devices may also be used for the display 216, and the invention is not limited to any particular type of display. As mentioned above, in one embodiment, a touch-screen display may be employed such that at least a portion of the functionality of the user input device 206 may be incorporated therein. Suitable displays may, for example, include any of a black & white, gray-scaled, or color LCD display, or an LCD bi-stable display.

As mentioned above, the use of the display 216, together with the user input device 206 (which may constitute the touch-screen functionality of the display 216) permits the Pocket Vault holder to flip or scroll through the various media stored in the memory 210 in much the same way as a person flips through the contents of his or her wallet. As mentioned above in connection with the description of the indicator 215, in addition to or in lieu of the display 216, other user output devices may also be employed

to provide information to the Pocket Vault holder. For example, light emitting diodes (LEDs), a beeper or buzzer, a speech synthesizer, a vibrator, etc., may be employed in some embodiments of the Pocket Vault 102.

The token port 218 of the Pocket Vault 102 may comprise a cavity or slot in which the token 102a is retained until it is released to be used to engage in a transaction, as well as the hardware employed to secure the token 102a in place when the token 102a has not been authorized to be released. In one embodiment, the token 102a stores a unique (and possibly encrypted) chip ID which is accessible to another device only when the token 102a is successfully released form the token port 218. In addition to the elements described above, the card port 218 may include additional hardware employed in connection with properly generating or configuring the token 102a prior to its release. This hardware is discussed in more detail below in connection with Fig. 6.

The fingerprint scanner 220 may comprise any device capable of accurately scanning a fingerprint of an individual for comparison with one or more fingerprint images stored in memory. The fingerprint scanner 220 may, for example, be a solid-state (non-optical) device. Devices that may be suitable for use as the fingerprint scanner 220 are available, for example, from Veridicom, Inc., of Santa Clara, California (www.veridicom.com), from Polaroid Corporation of Cambridge, Massachusetts (www.polaroid.com), and from Identix Incorporated of Sunnyvale, California (www.identix.com). The fingerprint scanner 220 may incorporate a temperature sensor that enables it to ensure that a live finger is contacting the scanning surface when the scanning function is employed. In addition to or in lieu of a fingerprint scanner, other bio-metric scanning devices may also be employed to verify the identity of the holder. For example, some embodiments may employ a charge coupled device (CCD) to serve as an iris or retina scanner, an optical sensor, and/or a voiceprint. Alternatively or additionally, a keystroke rhythm may be measured, either alone or in combination with another user authentication technique (e.g., a successful PIN code entry requirement), to validate the identity of the holder. The fingerprint scanner 220 and/or other bio-metric scanners may have touch pad capabilities built into them, thereby permitting them to constitute at least a part of the user input device 206 shown in Fig. 2.

Fig. 3 is a block diagram showing an example embodiment of one of the interface stations 104a-c shown in Fig. 1. The hardware employed to implement each of the stations 104a-c may be identical to the others or may be substantially different,

depending on the environment in which the station 104 is to be used, as well as the functional requirements of the particular station. Therefore, while the example embodiment described herein may be suitable for use as any of the stations, it should be appreciated that each of the stations may, in fact, be configured quite differently than the others.

As shown in Fig. 3, each interface station 104 may include both an the interface station computer 304 and a pocket vault interface unit 302. The interface station computer 304, for example, may be a standard desktop personal computer (PC), and may, as shown, comprise a controller 308, a user input device 318, a memory 320, a modem 322, and a display 324. These components are well known in the art and therefore will not be described in detail herein. The memory 320 of the interface station computer 304 may have instructions stored therein which, when executed by the controller 308, cause the controller to implement the routine described below in connection with Figs. 14-18 as well as any other software, e.g., a browser, drivers, etc., executing on the interface station computer 304.

The pocket vault interface unit 302 is coupled to the interface station computer 304 such that a controller 306 of the pocket vault interface unit 302 can communicate with the controller 308 of the interface station computer 304. The communications interface between these devices may, for example, comprise a Smartcard, Bluetooth or USB interface. As shown, in addition to the controller 306, the pocket vault interface unit 302 may comprise a transceiver 310, a docking interface 312, a finger print scanner 316, a stripe reader 315, and a memory 314. Further, although not shown in Fig. 3, the pocket vault interface unit 302 may also comprise a display and/or another device used to provide feedback to the operator, e.g., an audio indicator or LED.

The stripe reader 315 may be any conventional device for electronically reading the magnetic stripe on a token card such as a credit/debit card or drivers license. The stripe reader 315 may be used, for example, to read information from a token card so that such information can be downloaded to the network server 114 or the Pocket Vault 102.

The memory 314 may be any conventional memory suitable to store the software executed by the controller 306, as well as any data, e.g., stored fingerprint data, used in connection therewith. For example, the memory 314 of the pocket vault interface unit 302 may have instructions stored therein which, when executed by the controller 306,

cause the controller 306 to implement the routine described below in connection with Fig. 13.

As with the transceiver 204 of the Pocket Vault 102, the transceiver 310 of the pocket vault interface unit 302 may be any type of transceiver (or separate transmitter and receiver) capable of communicating with the other devices in the network 100 to enable the functionality described herein. For example, either an RF or an IR transceiver may be employed. Some embodiments may even include both an IR and an RF transceiver to be used in different applications. For example, an IR transceiver may be employed to interface the pocket vault interface unit 302 with a Pocket Vault 102, and a separate RF transceiver may be employed to communicate over a wireless network such as Bluetooth.

As with the docking interface 208 of the Pocket Vault 102, the docking interface 312 of the pocket vault interface unit 302 may take on any of numerous forms, and the invention is not limited to any particular type of interface device. The docking interface 312 may, for example, include a multi-pin plug adapted to mate with a receptacle used as the docking interface 208 of a Pocket Vault 102, or vice versa. The docking interface 312 may also comprise one or more implements (e.g., keys or grooves) to ensure that the plug or the like of the docking interface 208 of the Pocket Vault 102 mates correctly with the corresponding implement of the docking interface 312 when the Pocket Vault 102 and pocket vault interface unit 302 are physically mated together.

Finally, as with the fingerprint scanner 220 of the Pocket Vault 102, the fingerprint scanner 316 of the pocket vault interface unit 302 may comprise any device capable of accurately scanning a fingerprint of an individual for comparison with one or more fingerprint images stored in memory. The fingerprint scanner 316 may, for example, be a solid-state (non-optical) device. Devices that may be suitable for use as the fingerprint scanner 220 are available, for example, from Veridicom, Inc., of Santa Clara, California (www.veridicom.com), from Polaroid Corporation of Cambridge, Massachusetts (www.polaroid.com), and by Identix Incorporated of Sunnyvale, California (www.identix.com). The fingerprint scanner may incorporate a temperature sensor that enables it to ensure that a live finger is contacting the scanning surface when the scanning function is performed. In addition to or in lieu of a fingerprint scanner, other bio-metric scanning devices may also be employed to verify the identity of the interface station operator. For example, some embodiments may employ a charge

coupled device (CCD) to serve as an iris or retina scanner, an optical sensor, and/or a voiceprint. Alternatively or additionally, a keystroke rhythm may be measured, either alone or in combination with another user authentication technique (e.g., a successful PIN code entry requirement), to validate the identity of the operator. Although not shown, the pocket vault interface unit 302 may additionally comprise one or more user input devices enabling the operator to control or provide input to the pocket vault interface unit 302 or the software executing thereon. The fingerprint scanner 316 and/or other bio-metric scanners may, for example, have touch pad capability capabilities built into them, thereby permitting them to constitute such a user input device. Separate user input devices may also be employed.

Fig. 4 shows an example embodiment of the network server 114 shown in Fig. 1. As shown, the network server 114 may comprise one or more controllers 402, as well as a local memory 404, a database 406, and a transceiver 408 coupled thereto. The illustrated components of the network server 114 are well known, and therefore will not be described in detail. The transceiver 408 may, for example, be used to communicate with other devices in the network system 100 (Fig. 1) using a wireless network such as Bluetooth. The controller 404 may also communicate with other network devices via the Internet or a direct connection such as the type established using a dial up modem.

The local memory 404 may have instructions stored therein which, when executed by the controller 402, cause the controller 402 to implement the routines described below in connection with Figs. 19-25 and/or Figs. 30-39. In some embodiments, the local memory 404 and/or database 406 act as a website and execute software which may be accessed by a browser or similar software module operating on a computer. One such embodiment is described below in connection with Figs. 28-39.

The database 406 may, for example, comprise a relational database, and may be used to store the majority, if not all, of the data maintained by the network server 114. The database 406 may, for example, keep a real-time record of critical reference data along with transaction histories, back-up files, and security audit trail information for key events. Examples of specific items that may be stored in the database 406 include: a list of current Pocket Vault holders and appropriate contact information for each; records regarding the versions of software loaded onto each Pocket Vault 102, each pocket vault interface unit 302, and each interface station computer 304; a list of currently authorized or registered Pocket Vaults 102, identified by chip ID and linked to the holder list; a list

of currently authorized or registered tokens 102a, identified by chip ID and linked to the holder list; a list of currently authorized locations for interface stations 104 and telephone or other access lines therefor, including business information for each such location and an indication as to the type of interface station 104 it is (e.g., a validation interface station, a personal interface station, or a commercial interface station); a list of currently authorized or registered interface station operators and the interface stations 104 with which they are associated; a list of currently authorized or registered interface stations 104, identified by chip ID and linked to the list of authorized operators therefor, as well as encrypted cookie ID information (if any) for the respective interface stations 104; authorized media data received from media issuers that has not yet been downloaded to individual Pocket Vaults 102; backup data sets for individual Pocket Vault holders; detailed transaction histories for Pocket Vault registrations indicating where each Pocket Vault 102 was shipped from and to, where each Pocket Vault 102 was registered, which authorized interface station operator conducted the registration process, when that authorized operator was added to the list of authorized operators at a particular location, who submitted the key information to add the operator, which corporate representative associated with the network server 114 met with which representative associated with the interface station in establishing each new location for a validation interface station 104a, to whom and when each Pocket Vault 102 was issued; and communication encryption protocols. Each Pocket Vault account defined on the network server 114 may be defined to support multiple Pocket Vaults 102, as well as to identify other family members who may share certain contents of the Pocket Vaults 102 (e.g., family membership in a local museum).

The network server 114 may analyze data regarding consumer transactions, and thereby accumulate demographic information. Using this information, merchants, media issuers, and/or advertisers may, for example, define targeted marketing programs, which the network server 114 may then deliver to Pocket Vault holders that meet particular demographic profiles.

Fig. 5 shows how the memory 210 of the Pocket Vault 102 (Fig. 2) may be organized (conceptually) in accordance with one embodiment of the invention. The purpose of each of the illustrated memory components will be readily understood by those skilled in the art of the invention, and therefore will not be explained in detail.

Fig. 6 is a block diagram showing an example embodiment of the token 102a shown in Figs. 1 and 2. As shown, the token 102 may be equipped with a controller 602. In the embodiment shown, the controller 602 may be selectively programmed, for example, via interface terminals 606 to generate a current in a wire loop 608 so as to generate a magnetic field about the wire loop 608 that simulates a magnetic stripe of a standard credit card-like token. In other words, a magnetic field may be generated along the edge of the token 102a as if a magnetic stripe were present on that edge. The location of the simulated magnetic stripe on the token 102a is identified in Fig. 6 as a virtual magnetic stripe 610.

Appropriate software may be loaded onto the controller 602 (e.g., in an on-board memory of the controller 602) so as to enable the controller to generate the virtual magnetic stripe 610. When the token 102a is disposed in the token port 218, the terminals 606 of the token 102a may engage corresponding terminals of the token port 218, thereby enabling the controller 602 to be programmed appropriately. The programming of the controller 602 may be effected, for example, in response to commands from the controller 202 of the Pocket Vault 102, which commands may be generated in response to software executing on the controller 202.

As shown, the controller 602 may be powered by an appropriate resistor-capacitor (RC) circuit which stores a charge that decays over time. The RC circuit may be initially charged via the terminals 606 when the token 102a is disposed in the token port 218 and the controller 602 is being programmed. After the token 102a is removed from the token port 218, the controller 602 will remain powered only so long as sufficient charge remains stored by the RC circuit 604. Because the controller 602 can generate the virtual magnetic stripe 610 only when it is driven by an adequate power supply, the virtual magnetic stripe will disappear after the charge in the RC circuit 604 has decayed beyond a certain threshold level. Because the decay of an RC circuit is reasonably predictable, the virtual magnetic stripe 610 is disposed on the token 102a only for a finite, predetermined period of time after the token 102a is removed from the token port 218. In one embodiment, after the controller 602 loses power, the information with which it was programmed to enable it to generate the virtual magnetic stripe 610 is also lost. Therefore, the virtual magnetic stripe 610 of the token 102a cannot be used again until the controller 602 is again powered up and reprogrammed. Alternatively, the controller 602 may cut off the power to the wire loop 608 after a preset amount of time

or an amount of time determined by the Pocket Vault holder (possibly within preset limits). Additionally or alternatively, the token 102a may have its own embedded chip ID, which may be accessible only when the token 102a is successfully released form the token port 218.

In some embodiments, the token 102a may possess the characteristics of a bank-issued Smartcard, either in addition to or in lieu of the virtual magnetic stripe 610. Accordingly, the token 102a may include a specialized Smartcard chip or the controller 602 may be programmed to mimic such a chip. In any event, the token 102a may be preloaded with the bank's chip operating system (OS) and possibly customer-specific secure information. In such embodiments, the functionality of the Smartcard components may, for example, be enabled only in response to successful authentication of the Pocket Vault holder, e.g., using the fingerprint scanner 220 of the Pocket Vault 102. Therefore, the customer-specific "Smartcard" information may remain inaccessible so long as the Pocket Vault holder's identity has not been authenticated using the Pocket Vault 102.

In addition to or in lieu of the virtual magnetic stripe 610 and/or Smartcard components described herein, the token 102 may have disposed on it a conventional magnetic stripe that can be selectively written to by a magnetic read/write head in the Pocket Vault 102 before the token 102a is released from the token port 218. Like the other embodiments described above, the programming and/or use of such a token 102a could be restricted until after the identify of the Pocket Vault holder has been verified via biometric authentication, PIN code entry, or otherwise.

Moreover, in some embodiments, the token 102a may also have disposed on it a flexible LCD 612 or other suitable display mechanism or device. Prior to ejection of the token 102a from the token port 218, the Pocket Vault 102 may transfer information to the token 102a (e.g., via terminals 606) for display on the LCD 612. This transfer may either be direct or indirect (e.g., via a separate integrated circuit on the token 102a), and may involve the transfer of alphanumeric information (which may or may not include a hash code) and/or graphics, such as icons or barcodes. This information transferred may be encrypted, and de-encryption may be employed either in the separate integrated circuit on the token 102a or in a processor packaged with the LCD 612. In any event, the LCD 612 may receive the proper data to display, which

would match all or part of the code stored on the card by means of the virtual magnetic stripe 610, a writeable magnetic stripe, Smartcard simulation circuitry, etc.

In some embodiments, the LCD 612 may be powered by a capacitor configured and arranged to drain after a preset time, thereby rendering the LCD 612 inoperable until programmed again by the Pocket Vault 102. Thus, even if the token 102a were still swipeable or otherwise useable, a merchant could opt not to accept it because the requisite authorization information would not longer be displayed for certification purposes.

Instead of or in addition to an LCD or other type of display, some suitable technology may be employed to cause account information, and perhaps other information that is typically embossed or printed on credit cards or Smartcards, to appear temporarily on the token 102a after the token 102a is ejected from the token port 218. One technology that may be appropriate for this purpose is available from E-ink (www.Eink.com).

Thus, when an LCD display, a temporary ink technology, or the like, is employed on the token 102a, not only may the token 102a be selectively configured to have an actual or simulated magnetic stripe (or Smartcard personality) like a typical credit card or Smartcard, but it also may be configured to display information that is typically embossed or printed on such cards, including security enhancing information.

When used by a consumer, retailers may verify authenticity by matching the information displayed on the token 102a with that revealed in the swipe or other token reading process. Without a match, the token 102a may be rejected.

As discussed above, in some embodiments of the Pocket Vault 102, the transceiver 204 (Fig. 2) may be used as the transmitter and receiver of an RFID transponder, and thereby function as an RFID tag. Such an RFID tag may be selectively configured to have one of several personalities and may be rendered operable only when the holder of the Pocket Vault 102 authenticates his or her identity (e.g., in response to an accurate fingerprint scan by fingerprint scanner 220).

To appreciate the manner in which the Pocket Vault 102 may achieve this functionality, a prior art RFID tag system (shown in Fig. 41) will be briefly described. An RFID system includes at least one "RFID tag" and at least one "interrogator." The interrogator communicates with the RFID tag via an RF signal at some suitable frequency, e.g., somewhere between 10 kilohertz and about 5 gigahertz. The distance

between the RFID tag and the interrogator can be as short as near contact or as far as tens of feet away, depending upon the specific technology used. In most applications the RFID tag is a sealed device with no displays or user controls. The interrogator can be a hand held device that is manually operated or can be automated and included in a piece of stationary equipment, for example, at a parking garage, a toll booth, or a service station.

When the RFID tag comes within range of the interrogator, the two devices communicate in a session that may be a one-way read of the RFID tag information by the interrogator, or may be a two-way session in which the interrogator stores information in the RFID tag. The information stored in an RFID tag is typically an identification code such as a serial number. An RFID tag therefore functions much like a bar code, except that it is read by RF. To prevent counterfeiting, the information released from an RFID tag may be signed with a one-way cryptographic key so that it is difficult to decode or duplicate the code.

There are four possible types of RFID tags: (1) active, read only RFID tags, (2) passive, read only RFID tags, (3) active, read/write RFID tags, and (4) passive, read/write RFID tags. Read only RFID tags have information that is stored in them at time of manufacture and can only be read (and not written to) by the interrogator. A Read/Write tag might include a mix of read only information but will have some memory in the tag that can be altered by the interrogator. A passive tag has no battery or other permanent energy source. An active tag, on the other hand, has a battery or is plugged into an external energy source.

An example of a prior art RFID tag 4100 is shown in Fig. 41. As shown, the RFID tag 4100 is a self-contained electronic device that includes a receiver 4102a and a transmitter 4102b that share an antenna 4104 and are connected to a micro-controller 4106. The micro-controller 4106 is further connected to either a read-only memory 4108a or a read/write memory 4108b. The RFID tag 4100 is powered by rectifying the RF energy supplied to the antenna 4104 by the interrogator (not shown). If the RFID tag 4100 were of the "active" type, then an internal battery (not shown) would be employed.

In operation, when the RFID tag 4100 receives an interrogation signal from an interrogator (not shown) via the antenna 4104 and receiver 4102a, the micro-controller 4106 retrieves the tag's serial number from the memory 4108 and passes it to the transmitter 4102b and antenna 4104 for RF transmission to the interrogator. When a

read/write memory 4108b is employed, the micro-controller 4106 may also write information received from the interrogator to that memory.

In addition to typical electronic transponders such as that shown in Fig. 41, there also exist some RFID technologies that use non-electronic RFID tags. For example, interrogators can gather information from some types of RFID tags based solely on some physical property of the tags. For example, each RFID tag may employ several variable length antennas on a dielectric substrate, so that the interrogator can detect the length of the antennas present by sweeping through a range of frequencies. The specific pattern of antennas on the substrate thereby forms a unique code that can be recognized by the interrogator. Yet another approach is to use a surface acoustic wave (SAW) filter in which a surface electrode pattern determines a particular code that can be read by an interrogator.

Once programmed, the prior art RFID tag 4100 performs a single, dedicated function, namely, to release a serial number stored in memory 4108 in response to an interrogation signal, and there exists no control over who can use it for that purpose. In contrast, in some embodiments of the present invention, an RFID tag is provided wherein the personality of the tag, e.g., the code that is released upon interrogation, can be selected by the user from a number of possible personalities, and/or wherein the RFID tag can be rendered operational only by authorized users.

An example embodiment of an RFID tag system 4200 configured in accordance with this aspect of the invention is shown in Fig. 42. As shown, the system 4200 may include an RFID tag 4202 that is identical to the prior art RFID tag 4100, except that memory 4108 of the prior art device has been bypassed or replace by an I/O connection 4204 to the Pocket Vault 102. In such an embodiment, the Pocket Vault 102, rather than the memory 4108, can supply the information to the micro-controller 4106 of the RFID tag 4202 that is to be released to the interrogator (via the transmitter 4102b and antenna 4104) in response to an interrogation signal from the interrogator.

Accordingly, in such an embodiment, the information that is to be released by the RFID tag 4202 in response to an interrogation signal may be controlled by the holder of Pocket Vault 102. The Pocket Vault's holder may therefore select the personality to be taken on by the RFID tag 4202, for example, by using the user input device 206 (Fig. 2) to scroll through various personalities for the RFID tag 4202 that are displayed on the display 216, much like the holder is able to select a desired personality that is to be taken

on by the token 102a. The holder of the Pocket Vault 102 could therefore, for example, at one time select a "FastLane" personality for the RFID tag 4202, enabling the RFID tag to respond to an interrogator at a toll booth, and then at another time select a "Mobile Speedpass" personality, enabling the RFID tag to respond to an interrogator at a Mobile Service Station.

In some embodiments, at least some aspects of the RFID functionality of the Pocket Vault 102 may be exploited only after the identity of the Pocket Vault holder has been authenticated, e.g., using the fingerprint scanner 220 or by proper PIN code entry, thereby providing a level of security for RFID tags that has not heretofore been provided. The Pocket Vault 102 may, of course, permit some non-secure RFID personalities to be taken on by the RFID tag 4202 even without holder authentication.

In some embodiments, the data passed to the RFID tag 4202 can be made to be dependent not just on the recognition of a fingerprint, but based on an actual number tied to a feature extracted from the fingerprint. For example, the area of the finger may be such a feature. The number may then be used as a seed to a cryptographic code generator that creates the data to be sent to the RFID tag 4202.

In the embodiment shown in Fig. 42, the I/O connection 4204 between the Pocket Vault 102 and the RFID tag 4202 may be established in any of a number of ways and the invention is not limited to any particular mechanism or technique for establishing such a connection. In some embodiments, for example, the controller 202 of the Pocket Vault 102 may communicate with the micro-controller 4106 of the RFID tag 4202 via a cable connected between serial or parallel ports on the two devices. Alternatively, the two devices may be directly mated to one another in some suitable manner, or may communicate wirelessly if suitable security precautions are taken. The docking interface 208 of the Pocket Vault 102 may even provide a suitable mechanism for mating the two devices.

In some embodiments, the Pocket Vault 102 may have a separate memory (not shown in Fig. 2) dedicated to the storage of the RFID tag personality that is to be taken on by the RFID tag 4202, and the I/O connection 4204 may give the micro-controller 4106 of the RFID tag 4202 access to that memory. Alternatively, as mentioned above, the personality of the RFID tag 4202 may be communicated directly from the controller 202 of the Pocket Vault 102 to the micro-controller 4106 of the RFID tag 4202 via the I/O connection 4204.

The functionality of the RFID tag 4202 may additionally or alternatively be built directly into the Pocket Vault 102 (Fig. 2), rather that existing as a separate item. In some embodiments, for example, the functionality of the transceiver 4102 and micro-controller 4106 of the RFID tag 4202 may be embodied by the transceiver 204 and the controller 202 of the Pocket Vault 102. Alternatively, the Pocket Vault 102 may include a separate micro-controller, transceiver and/or memory dedicated to the RFID functionality discussed above. In yet another alternative embodiment, the functionality of the RFID tag 4202 may be embodied on the token 102a or on different device that may be selectively released from the housing of the Pocket Vault 102. The token 102a or other releasable device may, for example, include a memory that stores a selected personality for an RFID tag for only a predetermined, finite period of time, and then goes blank.

In some embodiments, the Pocket Vault 102 may also control the content of RFID tags that do not use an electronic circuit. This control can be accomplished in a number of different ways, and the invention is not limited to the use of any particular technique. In one embodiment, for example, the Pocket Vault 102 may activate one or more switches to short out one or more antennas, thereby changing the RFID code represented by them. As with the other embodiments, this selective configuration of an RFID tag may at least in certain circumstances be permitted only after proper authentication of the Pocket Vault holder's identity.

It should be appreciated that the RFID functionality discussed above need not be combined with some or all of the other aspects of the Pocket Vault 102. For example, some embodiments of the invention may comprise simply an RFID tag for which one of several personalities can be selected by the user, and/or an RFID tag that is selectively enabled only following proper user authentication, e.g., using a fingerprint scanner or PIN code entry.

As mentioned above, Figs. 7-12 are flow diagrams illustrating an example implementation of software that may be executed by the controller 202 of the Pocket Vault 102. As described below, this or additional proprietary software may enable menu structures, handle preference management, provide the data on and safeguard the programmability of the virtual magnetic stripe 610 (if so equipped), and ensure proper encryption data management. In one embodiment, local software for each Pocket Vault

102 and pocket vault interface station 104 may be upgraded from time to time by automatic download from the network server 114.

During execution of the routines of Figs. 7-12, various items may be displayed on the display 216, including prompts or icons regarding user input options (when a touch-screen display is employed as the display 216 or a point and click mechanism is employed herewith), and various items may also be displayed on the token 102a when the token 102a is ejected from the token port 218 of the Pocket Vault 102. Figs. 26A-P show examples of how the display 216 and the token 102a may appear as the routines of Figs. 7-12 are executed, and therefore will be discussed in connection with the description of these routines.

Fig. 7 is a flow diagram illustrating an example implementation of a primary routine 700 that may be executed by the controller 202 of the Pocket Vault 102. Instructions for the routine 700 may be stored, for example, in the "applications" section 508 of the memory 210 of the Pocket Vault 102.

As shown, the routine 700 begins at a step 702, wherein it is determined whether the Pocket Vault holder has applied his/her fingerprint to the fingerprint scanner 220 of the Pocket Vault 102. At the step 702, the display 216 of the Pocket Vault 102 may appear as shown in Fig. 26A. That is, the display 216 may be blank at the step 702, as the Pocket Vault 102 is currently powered down.

When, at the step 702, it is determined that the holder has applied his/her fingerprint to the fingerprint scanner 220, the routine 700 proceeds to a step 704, wherein the power manager 214 powers on the Pocket Vault 102. The routine 700 otherwise waits at the step 702 until the Pocket Vault holder has applied a fingerprint to the fingerprint scanner 220. Is should be appreciated, however, that, in some embodiments, the step 702 may not represent an instruction set executed by the processor 202. Instead, the step 702 may represent the detection of the occurrence of a physical action, e.g., the activation of a hardware switch, and the power manager 214 may be activated in response to the detection of such an action, without requiring intervention by the processor 202.

After the step 704, the routine 700 proceeds to a step 706, wherein the fingerprint scanner 220 scans the applied fingerprint of the Pocket Vault holder.

After the step 706, the routine 700 proceeds to a step 708, wherein it is determined whether the Pocket Vault 102 has been validated. In one embodiment, the

Pocket Vault 102 is not validated until: (1) a user's fingerprints have been stored in the fingerprint memory (e.g., the write-once memory 212 of Fig. 2), and (2) the Pocket Vault 102 has received and stored encrypted validation information (e.g., a PKI certificate) from the network server 114, as described below.

When, at the step 708, it is determined that the Pocket Vault 102 has not yet been validated, the routine 700 proceeds to a step 710, wherein a PROCESS POCKET VAULT VALIDATION routine (described below in connection with Fig. 8) is executed.

When, at the step 708, it is determined that the Pocket Vault 102 has already been validated, the routine 700 proceeds to a step 712, wherein it is determined whether Pocket Vault 102 has been authenticated, e.g., whether the fingerprint scanned at the step 706 matches one of the fingerprints stored in the fingerprint memory 212.

When, at the step 712, it is determined that the Pocket Vault has not been properly authenticated, the routine 700 proceeds to a step 714, wherein an UNAUTHORIZED HOLDER routine (discussed below in connection with Fig. 9) is executed. Figs. 26B-D show how the display 216 of the Pocket Vault 102 may appear during the UNAUTHORIZED HOLDER routine, and therefore are also discussed below in connection with Fig. 9.

When, at the step 712, it is determined that the Pocket Vault 102 has been properly authenticated, the routine 700 proceeds to a step 713, wherein an encrypted message including the unique Pocket Vault chip ID is transmitted to the pocket vault interface unit 302, in the event that the Pocket Vault 102 is interfaced or in communication with such a device.

In some embodiments, before a Pocket Vault holder is granted access to the contents of his or her Pocket Vault 102, a check may be made to ensure that the components used to interface the Pocket Vault 102 with the other components in the network 100 (either wirelessly or directly) are in place and operating correctly, and have not been compromised. Alternatively, the operability and integrity of such components may be checked just prior to their use.

Moreover, in some embodiments, prior to granting a holder access to the contents of the Pocket Vault 102, a check may be made to ensure that the contents of the Pocket Vault 102 have been updated recently. For example, the Pocket Vault 102 may forbid its holder from accessing its contents if the Pocket Vault 102 has not been updated at least

48 hours (or some other specified time period) prior to the attempted use. Updating of the Pocket Vault 102 may be accomplished, for example, using the synchronization or backup and recovery methods described herein.

After the step 713, the routine 700 proceeds to a step 716, wherein it is determined whether the Chameleon Card (i.e., the token 102a) is presently on-board the Pocket Vault 102 (i.e., whether the token 102a is disposed within the card port 218 of Fig. 2).

When, at the step 716, it is determined that the token 102a is not on-board the Pocket Vault 102, the routine 700 proceeds to a step 718, wherein the Pocket Vault holder is informed that the Chameleon Card is not on board, and is asked whether he/she wants to engage in a non-card transaction (i.e., a transaction not involving the token 102a).

After the step 718, the routine 700 proceeds to a step 720, wherein it is determined whether the holder has selected to engage in a non-card transaction.

When, at the step 720, it is determined that the holder has selected not to engage in a non-card transaction, routine 700 returns to the step 716 (described above), wherein it is again determined whether the Chameleon Card is on board the Pocket Vault 102. Therefore, the holder is permitted to engage in a transaction involving the Chameleon Card only when it has been confirmed that the Chameleon Card is on board the Pocket Vault 102.

When, at the step 720, it is determined that the holder has selected to engage in a non-card transaction, the routine 700 proceeds to the step 722, wherein the AUTHORIZED HOLDER routine (discussed below in connection with Figs. 10 and 11) is executed.

When, at the step 716, it is determined that the Chameleon Card is on-board the Pocket Vault 102, the routine 700 also proceeds to the step 722, wherein the AUTHORIZED HOLDER routine (discussed below in connection with Figs. 10 and 11) is executed. Figs. 26G-N and 26P show how the display 216 of the Pocket Vault 102 and the token 102a ejected therefrom may appear (when employed) during the AUTHORIZED HOLDER routine, and therefore are also discussed below in connection with Figs. 10 and 11.

After each of the steps 710, 714, and 720 (only one of which is executed during each iteration of the routine 700), the routine 700 proceeds to a step 724, wherein the

VERIFY CARD RETURN routine (discussed below in connection with Fig. 12) is executed. Fig. 26O shows how the display 216 of the Pocket Vault 102 may appear during the VERIFY CARD RETURN routine, and therefore is also discussed below in connection with Fig. 12.

After the step 724, the routine 700 proceeds to a step 726, wherein the screen of the display 216 is caused to flash to indicate that the Pocket Vault 102 is being shut down.

After the step 726, the routine 700 proceeds to a step 728, wherein the Pocket Vault 102 is powered down.

After the step 728, the routine 700 returns to the step 702, wherein the Pocket Vault 102 again waits for a fingerprint to be applied to the fingerprint scanner 220, and wherein the display 216 may again appear as shown in Fig. 26A.

Fig. 8 is a flow diagram illustrating an example embodiment of the PROCESS POCKET VAULT VALIDATION routine shown in Fig. 7 (step 710).

As shown, the routine 710 begins at a step 801, wherein the holder is informed (e.g., on the display 216) that the Pocket Vault 102 is not currently validated, and that the holder must interface the Pocket Vault 102 with an interface unit 302 of an appropriate interface station 104 (e.g., a validation interface station 104a) if the holder desires to validate the Pocket Vault 102.

After the step 801, the routine 710 proceeds to step 802, wherein it is determined whether the Pocket Vault 102 has been interfaced with an appropriate interface unit 302.

When, at the step 802, it is determined that the pocket vault 102 has not yet been interfaced with an appropriate interface unit 302, the routine 710 returns to the step 801 (discussed above).

When, at the step 802, it is determined that the Pocket Vault 102 has been interfaced with an appropriate interface unit 302, the routine 710 proceeds to a step 803, wherein it is determined whether the fingerprint memory, e.g., the write-once memory 212, is empty.

When, at the step 803, it is determined that the fingerprint memory is empty, the routine 710 proceeds to a step 804a, wherein the holder is prompted to apply a fingerprint from one finger of his or her left hand to the fingerprint scanner 220, waiting for a "beep" to be emitted (e.g., by indicator 215) after each fingerprint application.

Next, during steps 806a – 810a, the routine proceeds until the fingerprint of the selected finger has been scanned three times successfully.

After the steps 806a-810a, the routine proceeds to a step 804b, wherein the holder is prompted to apply a fingerprint from one finger of his or her right hand to the fingerprint scanner 220, waiting for a "beep" to be emitted (e.g., by indicator 215) after each fingerprint application.

Next, during steps 806b – 810b, the routine proceeds until the fingerprint of the selected finger has been scanned three times successfully.

After completing the steps 806b-810b, when a total of six fingerprints have been stored in memory, the routine 710 proceeds to a step 812, wherein an encrypted message including the pocket vault ID is transmitted to the interface unit 302, for ultimate transmission to the network server 114.

When, at the step 803, it is determined that the fingerprint memory, e.g., the write-once memory 212, is not empty, the routine 710 proceeds to a step 811, wherein it is determined whether the fingerprint scanned at the step 706 (Fig. 7) matches one of the stored fingerprints.

When, at the step 811, it is determined that the fingerprint scanned at the step 706 does match one of the stored fingerprints, the routine 710 proceeds to the step 812 (discussed above).

When, at the step 811, it is determined that the fingerprint scanned at the step 706 does not match any of the stored fingerprints, the routine 710 proceeds to a step 818, wherein an indication (e.g., a message on the display 216 or an audio signal from the indicator 215) is generated to inform the holder that the validation attempt was unsuccessful.

After the step 818, the routine 710 terminates.

After the step 812, the routine 710 waits at steps 814 and 816 to determine whether an encrypted message including validation information (e.g., a PKI certificate) has been received from the interface unit 302. This encrypted validation information may, for example, be received by the Pocket Vault 102 via either the docking interface 208 or the transceiver 204 of the pocket vault interface unit 302 of a validation interface station 104a. As discussed in more detail below, this encrypted validation information may, for example, be generated by the network server 114 and forwarded to the pocket vault interface unit 302 of a validation interface station 104a (via the interface station

computer 304 of the validation interface station 104a) after certain conditions have been met. The network server 114 may therefore ultimately determine whether each Pocket Vault 102 is permitted to receive this validation information.

When, at the step 816, it is determined that the time-out period has elapsed, the routine 710 proceeds to the step 818 (discussed above).

When, at the step 814, it is determined that encrypted validation information has been received before the timeout period of the step 816 has elapsed, the routine 710 proceeds to a step 820, wherein the validation information is stored in memory.

After the step 820, the routine 710 proceeds to a step 822, wherein an indication (e.g., a message on the display 216 or an audio signal from the indicator 215 of the Pocket Vault 102) is generated to inform the holder that the Pocket Vault 102 has been successfully validated.

After the step 822, the routine 710 terminates.

Fig. 9 is a flow diagram illustrating an example implementation of the UNAUTHORIZED HOLDER routine shown in Fig. 7 (step 714).

As shown, the routine 714 begins at a step 902, wherein a menu is displayed on the display 216 that permits the holder to select one of several options: (1) TRY AGAIN, (2) POCKET VAULT RETURN INFORMATION, (3) EMERGENCY INFORMATION, or (4) END SESSION. Fig. 26B shows how the display 216 may appear when the step 902 is reached. As shown, textual information and/or icons representing the various menu options may be displayed to the holder.

After the step 902, the routine 714 proceeds to a step 904, wherein the routine 714 waits for one of the displayed menu items to be selected by the holder (e.g., when the holder touches the location on the screen of the display 216 at which the menu item is displayed).

After one of the menu items has been selected at the step 904, the routine 714 proceeds to a step 906, wherein it is determined whether the TRY AGAIN option was selected. By selecting TRY AGAIN, the holder may request that the holder again be permitted to attempt to access the secure contents of the Pocket Vault 102 by reapplying the holder's fingerprint to the fingerprint scanner 220.

When, at the step 906, it is determined that the user has selected the TRY AGAIN option, the routine 714 proceeds to a step 912, wherein it is determined whether this is

the third sequential time that the scanned fingerprint has failed to match the fingerprint stored in memory.

When, at the step 912, it is determined that three sequential failed matches have occurred, the routine 714 proceeds to a step 914, wherein certain security precautions are taken in light of the multiple failed attempts to match the holder's fingerprint with that stored in the Pocket Vault 102. For example, when multiple failed matches have occurred, the Pocket Vault's secure memory may be erased, a security alert message may be broadcast by the transceiver 204 and/or any other prudent steps may be taken to ensure that an unauthorized user does not access the Pocket Vault's sensitive contents.

After the step 914, the routine 714 terminates.

When, at the step 912, it is determined that this is not the third consecutive time that the holder's fingerprint has failed to match that stored in the Pocket Vault's memory, the routine 714 terminates, and the holder may then again attempt (at the step 702) to access the Pocket Vault 102 by reapplying his/her fingerprint to the fingerprint scanner 220.

When, at the step 906, it is determined that the TRY AGAIN option has not been selected, the routine 714 proceeds to a step 908, wherein it is determined whether there exist any nested menu items for the menu item selected at the step 904.

When, at the step 908, it is determined that nested menu items do exist for the selected menu item, the routine 714 proceeds to a step 910, wherein the nested menu items for the selected menu item are displayed to the holder on the display 216.

After the step 910, the routine 714 returns to the step 904, wherein the routine 714 again waits for the holder to select one of the displayed menu items.

When, at the step 908, it is determined that no nested menu items exist for the selected menu item, the routine 714 proceeds to a step 916, wherein it is determined whether the END SESSION option has been selected.

When, at the step 916, it is determined that the END SESSION option has been selected, the routine 714 terminates.

When, at the step 916, it is determined that the END SESSION option has not been selected, the routine 714 proceeds to a step 918, wherein the information, if any, for the selected menu item is displayed to the holder on the display 216. Because the step 918 is reached only after a failed attempt to match the holder's fingerprint with that stored in the memory of the Pocket Vault 102, the information displayed at the step 918

may, for example, include information as to where the Pocket Vault 102 may be returned if it is found by someone other than the Pocket Vault holder (see Fig. 26C), or may be emergency information regarding the holder such as the holder's blood type, allergies, persons to contact in case of an emergency, etc. (see Fig. 26D). It should be appreciated that any of a number of non-secure media may be selected using the menu access routine discussed above in connection with steps 904-910, and may be displayed to the person accessing the Pocket Vault 102, regardless of the identity of that person. Of course, this non-secure information may be information that the holder would not mind falling into the hands of a stranger should the holder misplace or have his/her Pocket Vault 102 stolen.

After the step 918, the routine 714 proceeds to a step 920, wherein after a delay of a certain period of time (e.g., thirty seconds), the holder is prompted to reapply his/her fingerprint within a particular period of time (e.g., ten seconds) to avoid shut down of the Pocket Vault 102.

After the step 920, the routine 714 proceeds to a step 922, wherein it is determined whether a fingerprint has been reapplied to the fingerprint scanner 220 within ten seconds.

When, at the step 922, it is determined that a fingerprint has been reapplied to the fingerprint scanner 220 within ten seconds, the routine 714 returns to the step 918 (discussed above), wherein the selected information is again displayed to the user.

When, at the step 922, it is determined that a fingerprint has not been reapplied to the fingerprint scanner 220 within ten seconds, the routine 714 terminates.

Fig. 10 is a flow diagram illustrating an example implementation of the AUTHORIZED HOLDER routine of Fig. 7 (step 722).

As shown, the routine 722 begins at a step 1002, wherein it is determined whether an advertisement is scheduled for display on the Pocket Vault 102. Information regarding whether certain advertisements are to be displayed by the Pocket Vault 102 may have been uploaded, for example, from the personal interface station 104b in response to the holder previously interfacing the Pocket Vault 102 with the personal interface station 104b to synchronize the contents of the Pocket Vault 102 with information stored on the network server 114. The advertiser 108 (Fig. 1) may, for example, have made arrangements with the company operating the network server 114 to

have certain advertising information uploaded to Pocket Vaults 102 when particular Pocket Vault holders interface their Pocket Vaults 102 with their personal interface stations 104b.

When, at the step 1002, it is determined that an advertisement has been scheduled, the routine 722 proceeds to a step 1004, wherein the scheduled advertisement is displayed, for example, for approximately two seconds. Fig. 26I shows an example of how the display 216 may appear when such an advertisement is displayed.

After the step 1004, the routine 722 proceeds to a step 1006, wherein a "welcome screen" is displayed for a brief period (e.g., one second). Fig. 26G shows an example of how the display 216 may appear when such a welcome screen is displayed.

When, at the step 1002, it is determined that an advertisement is not scheduled, the routine 722 proceeds immediately to the step 1006, and no advertisement is displayed to the Pocket Vault holder.

After the step 1006, the routine 722 proceeds to a step 1008, wherein it is determined whether a "preferred" menu has been selected or pre-set for initial display to the Pocket Vault holder.

When, at the step 1008, it is determined that a preferred menu has been selected or pre-set, the routine 722 proceeds to a step 1012, wherein the display 216 fades to the preferred menu. Figs. 26H and 26J show examples of how the display 216 may appear when such a preferred menu is displayed. In the example of Fig. 26H, the preferred menu immediately shows the holder's preferred credit card as the selected menu item. Should the holder opt to use this media to engage in a transaction, the holder can simply choose the media directly. Alternatively, the holder may opt to access the HOME menu or other menu items by selecting appropriate icons displayed on the screen. In the example of Fig. 26J, the preferred menu immediately shows, perhaps, a selected group of the holder's most frequently used menu items.

When, at the step 1008, it is determined that a preferred menu has not been selected or pre-set, the routine 722 proceeds to a step 1010, wherein the display 216 fades to a standard HOME menu of secure items. Fig. 26L shows an example of how the display 216 may appear when the HOME menu is displayed.

After either one of the steps 1010 and 1012 has been executed, the routine 722 proceeds to a step 1014, wherein the routine 722 waits for the holder to select one of the displayed menu items.

When, at the step 1014, it is determined that the holder has selected a particular menu item, the routine 722 proceeds to a step 1016, wherein it is determined whether the holder has selected to enter or return to the HOME menu.

When, at the step 1016, it is determined that the holder has selected the HOME option, the routine 722 proceeds to the step 1010, wherein the HOME menu of secure items is displayed.

When, at the step 1016, it is determined that the holder has selected a menu item other than the HOME option, the routine 722 proceeds to a step 1018, wherein it is determined whether there exist any nested menu items for the selected menu item.

When, at the step 1018, it is determined that nested menu items do exist for the selected menu item, the routine 722 proceeds to a step 1020, wherein the nested menu items for the selected menu item are displayed. Thus, the holder may work his/her way through various layers of menu items until the desired menu item is reached. It should be appreciated that the menu items on the higher-level layers therefore may be categorized so as to enable the holder to quickly reach the desired media or other menu option.

When, at the step 1018, it is determined that no nested menu items exist for the selected menu item, the routine 722 proceeds to a step 1022, wherein it is determined whether the holder has selected a media from among the available menu items.

When, at the step 1022, it is determined that the holder has not selected a media, the routine 722 proceeds to a step 1040, wherein information relating to the selected non-media item may be displayed, or some other function may performed in accordance with the holder's selection. A non-media menu selection may involve, for example, preference settings for certain functional aspects of the Pocket Vault 102, e.g., whether the holder has a preferred secure menu (see step 1008). Preferences for the services or the device can be selected and, as appropriate, distributed to the Pocket Vault 102 either on the spot or the next time the Pocket Vault 102 is interfaced with an appropriate interface station 104. Preferences may, for example, include definition of home pages, connection of secure and non-secure media, order of media presentment, sort orders, user interface options, synchronization defaults, etc. Preferences that determine which items are displayed on the home page or on other pages may be defined. For example, a Pocket Vault holder may set up three preference sets: one for "business," one for "personal," and one for "vacation." The "personal" and "business" preference sets may

be set to be effective at different times of the day and/or different days of the week. The "vacation" preference set may be made effective for specific blocks of time determined by the Pocket Vault holder, possibly overriding the normal timing of the "personal" and "business" sets. The Pocket Vault holder may choose to establish the various preference settings based on his or her judgment or he or she may choose to allow the network server 114, supported by various databases, knowledge of the Pocket vault holder's various media and goals set by the Pocket Vault holder (e.g., minimize interest cost on credit cards or maximize frequent flyer miles, etc.), to determine optimal media use patterns and resulting media menu contents for a particular Pocket Vault holder. Preferences may also be defined between media that will link them for: (a) affiliate credits (like frequent flyer miles) that may be automatically presented to a merchant and tracked for a holder, (b) available discounts afforded by a membership (like senior citizen or AAA discounts), and/or (c) process improvement purposes (e.g., when information needs to be presented in a certain order to work properly). For example, a linkage preference may facilitate presentation of a discount card before presentation of a payment card when buying groceries.

After the step 1040, the routine 722 proceeds to a step 1042, wherein the holder is prompted either to END the session, or to return to the HOME menu.

After the step 1042, the routine 722 proceeds to a step 1044, wherein it is determined whether the holder has opted to END the session or to return to the HOME menu.

When, at the step 1044, it is determined that the holder has selected to return to the HOME menu, the routine 722 proceeds to the step 1010 (discussed above).

When, at the step 1044, it is determined that the holder has opted to END the session, the routine 722 terminates.

When, at the step 1022, it is determined that the holder has selected a media from the displayed menu items, the routine 722 proceeds to a step 1024, wherein the selected media is displayed to the holder on the display 216. The selected media may, for example, be a particular credit card, in which case the name of the credit card and/or the logo for the credit card and any preferred advertisement, specials, etc., for the selected media may be displayed to the holder as well.

After the step 1024, the routine 722 proceeds to a step 1026, wherein the holder is prompted to choose to: (1) EJECT the card, (2) to invoke a WIRELESS transaction, or (3) to return to the HOME menu.

After the step 1026, the routine 722 proceeds to a step 1028, wherein it is determined which of these three options has been selected by the holder.

When, at the step 1028, it is determined that the holder has opted to return to the HOME menu, the routine 722 proceeds to the step 1010 (discussed above).

When, at the step 1028, it is determined that the holder has selected the EJECT card option, the routine 722 proceeds to a step 1032, wherein it is determined whether the Chameleon Card is on board the Pocket Vault 102 (i.e., whether the token 102a is disposed in the token port 218).

When, at the step 1032, it is determined that the Chameleon Card is not on board the Pocket Vault 102, the routine 722 proceeds to a step 1034, wherein the holder is informed that the Chameleon Card is not on board the Pocket Vault 102.

After the step 1034, the routine 722 proceeds to the step 1026 (discussed above).

When, at the step 1032, it is determined that the Chameleon Card is on board the Pocket Vault 102, the routine 722 proceeds to a step 1036, wherein the PROCESS CARD TRANSACTION routine (discussed below in connection with Fig. 11) is executed.

After the step 1036, the routine 722 proceeds to a step 1038, wherein the VERIFY CARD RETURN routine (discussed below in connection with Fig. 12) is executed.

After the step 1038, the routine 722 proceeds to the step 1042 (discussed above).

When, at the step 1028, it is determined that the holder has opted to invoke a wireless transaction, the routine 722 proceeds to a step 1030, wherein the wireless transaction involving the selected media is executed. This wireless transaction may be invoked, for example, using the transceiver 204 of the Pocket Vault 102 to communicate with the transceiver 310 (Fig. 3) of a commercial interface station 104c (Fig. 1) over a wireless network, such as Bluetooth. Alternatively, the selected wireless transaction may be an RFID transaction if an RFID personality has been selected from amongst the available media. If such an RFID transaction has been selected, an appropriate RFID code may be supplied to the controller responsible for broadcasting an RF signal containing that code in response to an interrogation signal. If that controller is on the

Chameleon card, then these steps may alternatively be performed in connection with the PROCESS CARD TRANSACTION routine (step1036) discussed below.

As mentioned above, in embodiments that permit wireless transactions, a check of the wireless components may be made (e.g., verifying that an internal antenna (not shown) is in place and connected, and that related circuitry is not defeated or compromised in any way), prior to granting the holder access to the contents of the Pocket Vault 102. Alternatively, such a check may be made in response to such a wireless transaction being requested, e.g., at the step 1030.

After the step 1030, the routine 722 proceeds to the step 1042 (discussed above).

Fig. 11 is a flow diagram illustrating an example implementation of the PROCESS CARD TRANSACTION routine of Fig. 10 (step 1036).

As shown, the routine 1036 begins at a step 1102, wherein the Chameleon Card is configured to carry the selected media, and is ejected from the card port 218 (Fig. 2). As discussed above, the token 102a may be configured to carry the selected media in any of a number of ways, and the invention is not limited to any particular type of configuration technique. The card may be configured, for example, by using a magnetic read/write head to write to a conventional magnetic stripe on the token 102a, by causing the token 102a to generate a simulated magnetic stripe, by causing the token 102a to have a bar code disposed on it, and/or simply by causing a card number and perhaps security-related information to be visibly displayed it (e.g., using an LCD display or some type of printing technique). The token 102a may possibly be configured to hold such information for only a predetermined, finite period of time, so that it is not useable after such time. It should be appreciated, of course, that the card need not be temporarily configured in all embodiments, and may alternatively be configured in a more permanent manner in some embodiments.

After the step 1102, the routine 1036 proceeds to a step 1104, wherein the selected media is grayed out on the display 216 to indicate that the media is currently in use by the Chameleon Card. When the selected media is grayed out, the Pocket Vault's ability to configure another Chameleon Card with the grayed out media may also be disabled. Therefore, in such an embodiment, even if the Pocket Vault holder had an additional Chameleon Card available, the Pocket Vault 102 would be incapable of loading that media onto that Chameleon Card.

After the step 1104, the routine 1036 proceeds to a step 1106, wherein it is determined whether the selected media has stored value associated with it. The selected media may, for example, represent a pre-paid calling card from which value is deducted each time the media is used in a particular transaction, or a frequent flier card to which value (e.g., miles) is added in connection with each airline ticket purchased.

When, at the step 1106, it is determined that the selected media does have stored value associated with it, the routine 1036 proceeds to a step 1108, wherein a "stored value flag" (discussed below in connection with step 1126 of routine 1036 (Fig. 11) and step 1212 of routine 724 (Fig. 12)) is set to TRUE.

After the step 1108, the routine 1036 proceeds to a step 1110, wherein it is determined whether the holder has set a default option so as to permit the holder to maintain expense records by recording transactions into registers assigned to expense categories.

When, at the step 1106, it is determined that the selected media does not have stored value associated with it, the routine 1036 proceeds immediately to the step 1110.

When, at the step 1110, it is determined that the holder has not opted for the ability to maintain expense records, the routine 1036 terminates.

When, at the step 1110, it is determined that the holder has opted for the ability to maintain expense records, the routine 1036 proceeds to a step 1112, wherein the holder is prompted to decide whether to record the currently-pending transaction.

After the step 1112, the routine 1036 proceeds to a step 1114, wherein it is determined whether the holder has opted to record the pending transaction.

When, at the step 1114, it is determined that the holder has not opted to record the transaction, the routine 1036 terminates.

When, at the step 1114, it is determined that the holder has opted to record the transaction, the routine 1036 proceeds to a step 1116, wherein a menu including a number of options involving expense categories are displayed to the holder on the display 216.

After the step 1116, the routine 1036 proceeds to a step 1118, wherein the routine 1036 waits for the holder to select one of the displayed menu options.

When, at the step 1118, it is determined that the holder has selected a menu item, the routine 1036 proceeds to a step 1120, wherein it is determined whether the holder

selected the SKIP RECORD option, e.g., when the holder has changed his or her mind and opted not to record a particular transaction.

When, at the step 1120, it is determined that the holder has selected the SKIP RECORD option, the routine 1036 terminates.

When, at the step 1120, it is determined that holder has not selected the SKIP RECORD option, the routine 1036 proceeds to a step 1122, wherein it is determined whether any nested menu items exist for the selected menu item.

When, at the step 1122, it is determined that nested menu items do exist for the selected menu item, the routine 1036 proceeds to a step 1124, wherein the nested menu items are displayed to the holder on the display 216.

After the step 1124, the routine 1036 returns to the step 1118 (discussed above).

When, at the step 1122, it is determined that no nested menu items exist for the selected menu item, the routine 1036 proceeds to a step 1126, wherein it is determined whether the stored value flag was set to TRUE at the step 1108 (discussed above).

When, at the step 1126, it is determined that the stored value flag is set to TRUE, the routine 1036 proceeds to a step 1128, wherein a "record stored value transaction" flag (discussed below in connection with step 1216 of routine 724 (Fig. 12)) is set to TRUE.

After the step 1128, the routine 1036 terminates.

When, at the step 1126, it is determined that the "stored value" flag is not TRUE, the routine 1036 proceeds to a step 1130, wherein the holder is prompted to enter a dollar amount to be recorded for the transaction.

After the step 1130, the routine 1036 proceeds to a step 1132, wherein the routine 1036 waits for the holder to enter a transaction amount. After the holder has entered a transaction amount, the routine 1036 proceeds to a step 1134, wherein a "transaction summary approval" menu is displayed to the holder on the display 216. In the example shown, this menu permits the holder to select (1) to APPROVE the recordation, (2) to change the expense CATEGORY for the transaction, or (3) to change the AMOUNT to be recorded.

After the step 1134, the routine 1036 proceeds to a step 1136, wherein it is determined which of the menu items displayed in step 1134 the holder has selected.

When, at the step 1136, it is determined that the holder has selected to change the transaction AMOUNT, the routine 1036 returns to the step 1130 (discussed above).

When, at the step 1136, it is determined that the holder has opted to change the expense CATEGORY, the routine 1036 returns to the step 1116 (discussed above).

When, at the step 1132, it is determined that the holder has opted to APPROVE the recordation, the routine 1036 proceeds to a step 1138, wherein the entered transaction amount is added to the expense register for the selected category, and the balances associated therewith are updated accordingly.

After the step 1138, the routine 1036 terminates.

Fig. 12 is a flow diagram illustrating the VERIFY CARD RETURN routine of Fig. 7 (step 724).

As shown, the routine 724 begins at a step 1202, wherein it is determined whether the Chameleon Card is currently on board the Pocket Vault 102 (i.e., whether the token 102a is disposed within the token port 218).

When, at the step 1202, it is determined that the Chameleon Card is not on board the Pocket Vault 102, the routine 724 proceeds to a step 1204, wherein the holder is prompted to return the Chameleon Card to the token port 218 (see Fig. 260).

After the step 1204, the routine 724 proceeds to a step 1206, wherein it is determined whether a timeout period (e.g., ten seconds) has elapsed since the user was last prompted to return the Chameleon Card to the token port 218.

When, at the step 1206, it is determined that the timeout period has not yet elapsed, the routine 724 returns to the step 1202 (discussed above).

When, at the step 1206, it is determined that the timeout period has elapsed, the routine 724 proceeds to a step 1208, wherein the user is again prompted to return the Chameleon Card, this time with an audio indication (e.g., a "chime" sound generated by the indicator 215 of Fig. 2).

After the step 1208, the routine 724 proceeds to a step 1210, wherein it is determined whether an extended timeout period (e.g., 10 minutes) has elapsed since the user was first prompted to return the Chameleon Card to the token port 218.

When, at the step 1210, it is determined that the extended timeout period has not yet elapsed, the routine 724 returns to the step 1202 (discussed above).

When, at the step 1210, it is determined that the extended timeout period has elapsed, the routine 724 terminates.

When, at the step 1202, it is determined that the Chameleon Card is on board the Pocket Vault 102 (i.e., the token 102a is disposed within the token port 218), the routine

724 proceeds to a step 1212, wherein it is determined whether the "stored value" flag was set to TRUE in step 1108 of the routine 1036 (Fig. 11).

When, at the step 1212, it is determined that the "stored value" flag is not TRUE, the routine 724 terminates.

When, at the step 1212, it is determined that the "stored value" flag is TRUE, the routine 724 proceeds to a step 1214, wherein the stored value for the selected media is updated based on the amount deducted from the Chameleon Card during its use.

After the step 1214, the routine 724 proceeds to a step 1216, wherein it is determined whether the "record stored value transaction" flag was set to TRUE in the step 1128 of the routine 1036 (Fig. 11).

When, at the step 1216, it is determined that the "record stored value transaction" flag is FALSE, the routine 724 proceeds to a step 1222, wherein the "stored value" flag is set to FALSE.

When, at the step 1216, it is determined that the "record stored value transaction" flag is TRUE, the routine 724 proceeds to a step 1218, wherein the dollar amount of the transaction is added to the selected expense register (i.e., the expense register selected at the step 1118 of the routine 1036 (Fig. 11)). The dollar amount entered is determined based on the dollar amount that was deducted from the stored value on the Chameleon Card as a result of the transaction.

After the step 1218, the routine 724 proceeds to a step 1220, wherein the "record stored value transaction" flag is set to FALSE.

After the step 1220, the routine 724 proceeds to the step 1222 (discussed above)

After the step 1222, the routine 724 terminates.

In addition to a routine such as that discussed above in connection with Figs. 7-12, certain software enhancements may also be disposed in the memory 210 of a Pocket Vault 102 for use with the controller 202. One such software enhancement involves the use of "system preference file" software. This software may establish certain preferences that cannot be altered on the Pocket Vault 102 by the holder, and which may be stored in encrypted form, along with certain information regarding value-based media. For example, Pocket Vaults 102 may be sold with a choice of two or three advertising profiles. During the Pocket Vault registration and validation process (described below), an encrypted system preference file may be created that indicates whether the device was, for example, subject to a "Premium," "Plus" or "Base" profile status. This status

may have been selected, for example, on the Pocket Vault 102 itself, or using one of the interface stations 104a-c when the Pocket Vault 102 was interfaced therewith.

Under the "Premium" profile, the Pocket Vault 102 may be advertising-free, but cost a significant amount. Under the "Plus" profile, the Pocket Vault 102 may display only advertising related to shops or services you currently patronize, but cost significantly less than the "Premium" version. Under the "Base" profile, the Pocket Vault 102 may have a variety of advertising on a regular basis, subject only to network "saturation effectiveness" limitations, and the Pocket Vault 102 may be free, or nearly so (e.g., a small purchase charge to generate in-store revenue for the retailer may be charged).

A holder's choice about participation in specific promotional campaigns linked to the holder's buying behavior may also be part of the registration process and affect retail pricing. Once chosen, the network server 114 may send a message to the Pocket Vault 102, e.g., via the validation interface station 104a, and direct the storage of necessary encrypted information on the Pocket Vault 102 (e.g., "Buyer Profile Participant").

The advertising and marketing choices may be changed at a date after purchase and result in a changed set of costs (either credits or debits) to the Pocket Vault holder. Other system preference data may include the "saturation effectiveness" limitations on the amount of advertising that can appear during any given single use window (a particular period during which the device is powered on), any given hour, any given day and/or any given month. The limitations may control both the number of advertisements permitted and the amounts of advertisement time permissible (e.g., seconds per advertisement), by category (e.g., such limitations may, for example, based on categories of advertisements be imposed general advertising, advertising from retailers that the Pocket Vault holder already patronizes and advisory notices from the network server 114. For example, these limits may be set to balance the need for advertising revenue with the need to not overwhelm or annoy Pocket Vault holders. This preference file may, for example, limit all advertising to one advertisement per "on-session," two advertisements per hour, four advertisements per day and/or twenty advertisements per month. General advertisements might get priority claim on this time up to a set limit (say 75% of all advertisement time), with targeted advertisements next, and advisory messages last.

Another software enhancement that may be employed is software used for preference file management. Such "preference file management" software may, for example, include a default file which is periodically updated from the network server 114, and a Pocket Vault holder custom file. Using this software, the holder may, for example, be able to modify: (1) the initial on-screen backdrop and message greeting; (2) the menu structure and media order within menu screens; (3) some (but not all) of the bio-metric input requirement parameters; (4) the amount of on-time after the bio-metric data is confirmed (within pre-set limits); (5) the ability to conceal all or part of the credit or debit account information on the Chameleon Card display area; (6) the normal restaurant tip percentage; (7) the links between certain media; and/or oversight preference restrictions.

For example, some of the menu tree structures for the Pocket Vault 102 may be set by the holder. This may include the sequence in which certain screens appear (e.g., debit screens before credit screens), among credit screens (e.g., Visa before MasterCard) and media order-of-appearance within a screen (e.g., FirstCard Visa before ChaseVisa).

Generally, a retailer does not need to see a credit or debit account number, while the approving entity contacted on the dialup modem does. Today, credit and debit cards have this information embossed on the card and recorded in the magnetic stripe on the back of the card. If the magnetically encoded information is unreadable due to mechanical wear of the magnetic stripe or for other reasons, the embossed image can always be read by the clerk and manually keyed in. There is no way for this embossing to disappear when it is not needed and appear at just the right time, either with a standard card or a Smartcard. As a result, such numbers are generally in view and this visibility may lead to fraud. In one embodiment, the Pocket Vault 102 may be programmed to conceal this number, unless prompted to the contrary by the holder. A retailer may confirm the kind of credit or debit being presented and the full name on the card, without having to see or be told the account number. On the rare occasion when the number itself is needed, the holder may, for example, repeat the bio-metric input to the Pocket Vault 102 to reveal the card account number. If placed in the personal interface station 104c, such account numbers may be automatically revealed (e.g., through detection of an encrypted cookie on the interface station computer 304 of the personal interface station 104c).

If the holder establishes a preferred tip percentage, this preferred tip amount may be automatically applied to restaurant checks. This may eliminate a step in restaurant check close-out and reduce the hassle of calculating an appropriate tip and eliminate the need for waitstaff to return to pick up the credit receipt with the tip.

The holder may also choose to link certain media on the Pocket Vault 102 to reduce selection tasks at the point-of-transaction. For example, the holder may link certain credit or debit cards to certain frequent buyer ID cards, thereby enabling the holder to pick a grocery store frequent buyer card (which would be linked to a debit card and brought up automatically after the grocery store card).

At the point of registration or issuance, a Pocket Vault holder may be asked if there is to be any transaction oversight security. If the answer is yes, a second bio-metric input may be required from the individual endowed with that oversight role. For example, a parent may choose to get a Pocket Vault 102 for a child or other relative who may lack certain fiscal discipline. At issuance, and prior to any credit or debit media being added to the Pocket Vault 102, the oversight authority may need to be established. The person having such oversight authority may then have sole access to a profile of transaction preference data. The person having the oversight authority may therefore create and modify this profile any time after issuance. This data set may limit one or more of the following: (1) debit and credit transaction dollar volume per day, per week and/or per month; (2) certain purchase restrictions such as the types of retailers to whom payments are permitted, such as exclusion of gambling establishments or liquor stores; and (3) geographic restrictions such as payments within 10 miles of a son's or daughter's college campus, but not beyond).

Another software enhancement that may be employed is software for managing media image libraries. Every media image sent to the display 216 may actually be a composite of from two to five layers of graphics files. Layers one, two and four may, for example, be stored in media library files while layers three and five may include text and data files stored in memory on the Pocket Vault 102. For example, a credit card image may comprise separate layers for: (1) the standard credit card background and icon; (2) the issuing bank's overlay icons and text; (3) the individual's account number; and (4) customized advertising from the issuing bank and/or credit card company.

Layering the image in this fashion may minimize data transmission requirements, reduce memory storage requirements, and speed up screen display. For example, Pocket

Vaults 102 may be preloaded at point of manufacture with background images of the top ten credit images, three passport images (e.g., EU, US, Japan), and a handful of other globally-relevant backgrounds. When, for example, a Pocket Vault holder living in Boston initially registers a device, it may trigger downloading of the top five additional background images prevalent in that area. When the individual applies for and is electronically issued a new credit card over the network system 100, the download from the network server 114 may include a second layer credit card company overlay for the credit card, along with the third layer of account and name information, and the fourth layer of the most recent customized advertisement from the credit card company related to a seasonal promotion of card usage.

The advertisement layer may be temporary in nature. This layer may, for example, remain on-screen for a given number of seconds, predetermined by the time period of the advertisement paid for by the advertiser. Underneath such an advertisement, a fifth layer of Pocket Vault holder-determined data may appear, also for a temporary period, in this case for privacy reasons and for a period set by the holder. This positioning of the holder's data below the advertising data increase the value of the advertisement time, since holders will be likely to view the display 216 awaiting the appearance of their data, which may also remain on-screen for only a set number of second. For example, such holder-specific data may include the last date of the next billing period, or the total charges since the last billing period on this particular card or on all of the holder's credit cards. Such balance information may be generated, for example, by the financial management software. The initial on-screen image may also be layered, for example, with a market-tailored backdrop and a sign-on message, both of which possibly being modifiable could be modified by the appropriate setting of user preferences.

Another software enhancement that may be employed is software to manage memos. Certain screen choices may, for example, result in the viewing of memos created by and for the Pocket Vault holder. These memos may be written on a home PC and transferred to a Pocket Vault 102 when the Pocket Vault 102 is interfaced with the personal interface station 104c for an update/download session. Alternatively, such memos may be created on the Pocket Vault 102 using a screen-based keyboard function similar to that of a Palm Pilot. The memo template software may provide certain

standard backgrounds and layouts to support this feature. This feature may help to eliminate the need for scraps of various notes now found in most wallets.

Yet another software enhancement that may be employed is software to manage advertising messages. Such advertising message management software may, for example, perform several noteworthy functions: (1) limiting the appearance of advertising in accordance with the advertising profile (e.g., stored in the network server 114) of the particular Pocket Vault holder; (2) limiting the appearance of advertising to a certain number of times per on-session, per hour, per day, per week and/or per month; (3) tracking the number of times each advertisement appears since the last download/update session (since the number of on-sessions during any period will govern the number of opportunities certain advertisements have to run, this tracking may be necessary to enable billing of advertisers for actual advertisement exposure levels; (4) generating reminder advertisements for frequent buyer cards (e.g., a message such as "Ten weeks since your last car wash! One more and the next is free!"); and (5) tracking the effectiveness of advertising through linkage to the transaction files (e.g., the ability to build more accurate, comprehensive buying profiles since all of an individual's media are now "under one roof").

Another software enhancement that may be employed is software to process transaction data. Such transaction processing software may, for example, include the ability to track total outstanding transactions on particular media and compare those to media limits at the time of the next transaction, along with date validity of the media. If a particular piece of media is no longer valid, selection of this item from a menu may produce a message such as "expired," or "requires update to extend period of validity," or "payment of balance required before re-use."

Another software enhancement that may be employed is software to manage frequent buyer data. Such frequent buyer data management software may, for example, track purchases at stores with frequent buying programs that participate in the network system 100. This software may also indicate any frequent buyer credits that are about to expire or create advertisements that remind their Pocket Vault holders that they are about to qualify for a free item. For example, a tenth gasoline purchase at a service station/car wash may generate a message indicating that the holder is "now entitled to free car wash."

Yet another software enhancement that may be employed is software for managing financial information. This type of software may, for example, enable easy download advertisements into personal finance software used by some PC owners. It may also support certain on-board functionality in the Pocket Vault, such as charge card management, automatically shifting from the preferred credit card to another credit card, for example: (1) when a transaction would cause a credit limit to be exceeded, (2) when using a different card would lengthen the time after which actual payment would be due, (3) when using another card would garner desired contest eligibility, or maximize cash back points for a particular period, and/or (4) when use of another card would preclude having to pay annual dues.

Another software enhancement that may be employed is Global Positioning Software. Integration of this functionality with memo information and frequent buyer information may induce visits to nearby stores at convenient times to take advantage of sales, frequent buyer credits, etc.

Fig. 13 is a flow diagram illustrating an example implementation of a primary routine 1300 that may be executed by the controller 306 of the pocket vault interface unit 302 (Fig. 3).

As shown, the routine 1300 begins at a step 1346, wherein it is determined whether a card has been swiped through the stripe reader 315 of the interface unit 302.

When, at the step 1346, it is determined that a card has been swiped, the routine 1300 proceeds to a step 1348, wherein information from the swiped card read by the stripe reader 315 is transmitted to the interface station computer 304.

After the step 1348, the routine 1300 proceeds to a step 1302, wherein it is determined whether a first encrypted message has been received from the Pocket Vault 102 including an ID code that is released from the Pocket Vault 102 only upon proper user authentication (e.g., in response to a fingerprint match).

When, at the step 1346, it is determined that a card has not been swiped, the routine 1300 proceeds directly to the step 1302 (discussed above).

When, at the step 1302, it is determined that such a first encrypted message has not been received from the Pocket Vault 102, the routine 1300 proceeds to a step 1338, wherein it is determined whether any encrypted information and/or commands have been received from the interface station computer 304.

When, at the step 1338, it is determined that information and/or commands have been received from the interface station computer 304, the routine 1300 proceeds to a step 1340, wherein the received information and/or commands are forwarded to the Pocket Vault 102.

After the step 1340, the routine 1330 proceeds to a step 1342, wherein it is determined whether any information and/or commands have been received from the Pocket Vault 102.

When, at the step 1338, it is determined that no information or commands have been received from the interface station computer 304, the routine 1300 proceeds directly to the step 1342 (discussed above).

When, at the step 1342, it is determined that information and/or commands have been received from the Pocket Vault 102, the routine 1300 proceeds to a step 1344, wherein the received information and/or commands are forwarded to the interface station computer 304.

After the step 1344, the routine 1300 returns to the step 1346 (discussed above).

When, at the step 1342, it is determined that no information and/or commands have been received from the Pocket Vault 102, the routine 1300 proceeds directly to the step 1346.

When, at the step 1302, it is determined that a first encrypted message including a Pocket Vault ID has been received from the Pocket Vault 102, the routine 1300 proceeds to a step 1304, wherein the first encrypted message is forwarded to the interface station computer 304 (Fig. 3).

After the step 1304, the routine 1300 proceeds to steps 1306 and 1308, wherein it is determined whether a fingerprint has been scanned by the fingerprint scanner 316 of the pocket vault interface unit 302 before a timeout period measured by the step 1308 has elapsed.

When, at the steps 1306 and 1308, it is determined that a fingerprint has not been scanned within the timeout period of step 1308, the routine 1300 returns to the step 1346 (discussed above).

When, at the steps 1306 and 1308, it is determined that a fingerprint has been scanned by the fingerprint scanner 316 in a timely manner, the routine 1300 proceeds to a step 1310, wherein it is determined whether the scanned fingerprint matches a fingerprint stored in the memory 314 of the pocket vault interface unit 302.

When, at the step 1310, it is determined that the scanned fingerprint does match that of an authorized operator of the interface unit 302, the routine 1300 proceeds to a step 1312, wherein a second encrypted message, including an ID of the pocket vault interface unit 302 that is released only after a successful fingerprint match, is transmitted to the interface station computer 304.

After the step 1312, the routine 1300 returns to the step 1346 (discussed above).

When, at the step 1310, it is determined that the scanned fingerprint does not match any fingerprint stored in the memory 314 of the pocket vault interface unit 302, the routine 1300 proceeds to a step 1314, wherein a message is transmitted to the interface station computer 304 indicating there has been an unsuccessful attempt to authenticate an operator of the pocket vault interface unit 302.

After the step 1314, the routine 1300 proceeds to steps 1316 and 1318, wherein it is determined whether, before the expiration of a timeout period measured by the step 1318, a request has been received from the interface station computer 304 to add a new operator to the pocket vault interface unit 302.

When, at the steps 1316 and 1318, it is determined that such a request has not been received from the interface station computer 304 in a timely manner, the routine 1300 returns to the step 1302 (discussed above).

When, at the steps 1316 and 1318, it is determined that a request to add a new operator to the pocket vault interface unit 302 has been received from the interface station computer 304 in a timely manner, the routine 1300 proceeds to steps 1320 and 1322.

At the steps 1320 and 1322, it is determined whether three identical fingerprints have been stored in the interface unit 302 for each of the operator's two hands before the expiration of a timeout period measured by the step 1322. The operator may be prompted, e.g., on the display 324 of the interface station computer 304, to take appropriate steps to ensure his or her fingerprints are properly scanned. An example routine for obtaining the requisite fingerprint data from a user is discussed above in connection with steps 804a-810a and 804b-810b (for the Pocket Vault 102), and therefore will not be repeated here.

When, at the steps 1320 and 1322, it is determined that the requisite fingerprint information has not been stored in a timely manner, the routine 1300 proceeds to a step

1336, wherein an indication (e.g., a message or an audio tone) regarding the unsuccessful new operator validation attempt is generated.

After the step 1336, the routine 1300 returns to the step 1346 (discussed above).

When, at the steps 1320 and 1322, it is determined that the fingerprint information has been successfully stored in the interface unit 302 in a timely manner, the routine 1300 proceeds to a step 1324, wherein an encrypted message including an ID unique to the interface unit 302 is transmitted to the interface station computer 304 for ultimate registration with the network server 114.

After the step 1324, the routine 1300 proceeds to step 1326 and 1328, wherein is determined whether a message including validation information (e.g., a PKI certificate for the interface unit 302) has been received from the network server 114 (via the interface station computer 304) before the expiration of a timeout period.

When, at the steps 1326 and 1328, the validation information is not received by the interface unit 302 in a timely manner, the routine 1300 proceeds to the step 1336 (discussed above).

When, at the steps 1326 and 1328, it is determined that the validation information is received by the interface unit 302 in a timely manner, the routine 1300 proceeds to a step 1330, wherein the validation information is stored for the new operator.

After the step 1330, the routine 1300 proceeds to a step 1332, wherein an indication (e.g., a message or an audio tone) regarding the successful validation of the new operator is generated.

After the step 1332, the routine 1300 returns to the step 1346 (discussed above).

Fig. 14 is a flow diagram illustrating example implementation of a primary routine 1400 that may be executed by the controller 308 of the interface station computer 304 of Fig. 3.

As shown, the routine 1400 begins at a step 1402, wherein a menu is displayed on the display 324 of the interface station computer 304 that gives the operator of the interface station computer 304 several options to choose from. These options may, for example, include: (1) the option to request that a Pocket Vault 102 be validated (i.e., permitted to store a new finger print), (2) the option to request that the information currently stored on a Pocket Vault 102 be updated (e.g., information may be uploaded from the network server 114), (3) the option to request that a transaction involving a

Pocket Vault 102 be authorized, and/or (4) the option to access a website on the network server 114 and take advantage of the functionality thereof.

It should be appreciated that the foregoing are only examples of menu options that may be provided to the operator of the interface station computer 304, and that the invention is not limited to the particular examples described. It should also be appreciated that fewer than all of the options shown may be provided in connection with different types of interface stations. For example, a validation interface station 104a may be provided only with option (1), a personal interface station may be provided only with option (2), and a commercial interface station may be provided only with option (3). In many instances, option (4) may be the only option required or desired to be employed by the user, as the website may itself provide all of the functionality of the other options (1)-(3). If fact, in such circumstances, the user need not be provided with a menu at all, as the user could simply log on the website using a browser. An embodiment of a network system in which a website may be accessed by a server in this manner is discussed below in connection with Figs. 28-39.

After displaying the menu at the step 1402, the routine 1400 proceeds to a step 1404, wherein it is determined whether any requests to validate Pocket Vaults 102 have been received.

When, at the step 1404, it is determined that no request to validate a Pocket Vault 102 has been received, the routine 1400 proceeds to a step 1408, wherein it is determined whether any requests to update information on Pocket Vaults 102 have been received.

When, at the step 1408, it is determined that no request to update the information on a Pocket Vault 102 has been received, the routine 1400 proceeds to a step 1412, wherein it is determined whether any requests to authorize transactions involving Pocket Vaults 102 have been received.

When, at the step 1412, it is determined that no request to authorize a transaction involving a Pocket Vault 102 has been received, the routine 1400 proceeds to a step 1416, wherein it is determined whether the interface station computer has received any messages from Pocket Vault interface units 302 indicating that an unsuccessful operator authentication has occurred (i.e., the fingerprint of an operator scanned by the fingerprint scanner 316 has failed to match a fingerprint stored in the memory 314).

When, at the step 1416, it is determined that no such messages have been received, the routine 1400 proceeds to a step 1420, wherein it is determined whether a request to access a website on the network server 114 has been received.

When at the step 1420, it is determined that no request to access the website on the network server 114 has been received, the routine 1400 returns to the step 1402, wherein the menu of the various options for the operator is again displayed. Thus, the menu 1402 is displayed until one of the various options is selected in accordance with any of the steps 1404, 1408, 1412, 1416, or 1420.

When, at the step 1404, it is determined that a request to validate a Pocket Vault 102 has been received, the routine 1400 proceeds to a step 1406, wherein the PROCESS REQUEST TO VALIDATE POCKET VAULT routine (discussed below in connection with Fig. 15) is executed.

After the step 1406, the routine 1400 proceeds to the step 1408 (discussed above).

When, at the step 1408, it is determined that a request to update the information on a Pocket Vault 102 has been received, the routine 1410 proceeds to a step 1410, wherein the PROCESS REQUEST TO UPDATE INFO ON POCKET VAULT routine (discussed below in connection with Fig. 16) is executed.

After the step 1410, the routine 1400 proceeds to the step 1412 (discussed above).

When, at the step 1412, it is determined that a request to authorize a transaction involving a Pocket Vault 102 has been received, the routine 1400 proceeds to a step 1414, wherein the PROCESS REQUEST TO AUTHORIZE TRANSACTION routine (discussed below in connection with Fig. 17) is executed.

After the routine 1414, the routine 1400 proceeds to the step 1416 (discussed above).

When, at the step 1416, it is determined that a message has been received from an the interface station computer 304 indicating that an attempted fingerprint match of an operator has failed, the routine 1400 proceeds to a step 1418, wherein the PROCESS UNSUCCESSFUL OPERATOR AUTHENTICATION routine (discussed below in connection with Fig. 18) is executed.

After the routine 1418, the routine 1400 proceeds to the step 1420 (discussed above).

When, at the step 1420, it is determined that a request to access a website on the network server 114 has been received, the routine 1400 proceeds to a step 1422, wherein

the PROCESS REQUEST TO ACCESS WEBSITE routine (discussed below in connection with Figs. 30-39) is executed.

After the step 1422, the routine 1400 returns to the step 1402 (discussed above).

Fig. 15 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO VALIDATE POCKET VAULT routine of Fig. 14 (step 1406).

As shown, the routine 1406 begins at a step 1502, wherein the potential new Pocket Vault holder is prompted to apply his or her fingerprint to the fingerprint scanner 220 of the Pocket Vault 102, and to interface the Pocket Vault 102 with the pocket vault interface unit 302. This may be accomplished, for example, by interfacing the docking interface 208 of the Pocket Vault 102 with the docking interface 312 of the pocket vault interface unit 302.

After the step 1502, the routine 1406 proceeds to steps 1504 and 1506, wherein it is determined whether an encrypted message including the ID of the Pocket Vault 102 has been received from the pocket vault interface unit 302 prior to the expiration of a timeout period measured by the step 1506.

When, at the steps 1504 and 1506, it is determined that an encrypted message including the ID of the Pocket Vault 102 has not been received from the pocket vault interface unit 302 in a timely manner, the routine 1406 proceeds to a step 1526, wherein a message is displayed on the display 324 of the interface station computer 304 indicating that an error has occurred in the Pocket Vault validation process.

When, at the steps 1504 and 1506, it is determined that an encrypted message including the ID of the Pocket Vault 102 has been received from the pocket vault interface unit 302 in a timely manner, the routine 1406 proceeds to a step 1506, wherein the interface station operator is prompted to apply his or her fingerprint to the fingerprint scanner 316 of the pocket vault interface unit 302.

After the step 1506, the routine 1406 proceeds to steps 1508 and 1510, wherein it is determined whether an encrypted message including the ID of the pocket vault interface unit 302 has been received from the pocket vault interface unit 302 prior to the expiration of a timeout period measured by the step 1510.

When, at the steps 1508 and 1510, it is determined that an encrypted message including the ID of the pocket vault interface unit 302 has not been received from the pocket vault interface unit 302 in a timely manner, the routine 1406 proceeds to the step

1526, wherein a message is displayed on the display 324 of the interface station computer 304 indicating that the attempt to authorize the interface station operator was unsuccessful.

After the step 1526, the routine 1406 terminates.

When, at the steps 1508 and 1510, it is determined that an encrypted message including the ID of the pocket vault interface unit 302 has been received from the pocket vault interface unit 302 in a timely manner, the routine 1406 proceeds to a step 1512, wherein the interface station operator is prompted to input information regarding the new Pocket Vault holder into the interface station computer 304.

After the step 1512, the routine 1406 proceeds to a step 1514, whereat the routine 1406 waits until all of the requisite information regarding the new Pocket Vault holder has been entered properly (e.g., via the user input device 318 of the interface station computer 304).

After the step 1514, the routine 1406 proceeds to a step 1516, wherein the network server 114 (Fig. 1) is contacted.

After the step 1516, the routine 1406 proceeds to a step 1518, wherein the information regarding the new Pocket Vault holder is transmitted to the network server 114, along with a request that the new Pocket Vault holder be validated.

After the step 1518, the routine 1406 proceeds to steps 1520 and 1522, wherein it is determined whether the network server 114 has acknowledged the request by the interface station computer 304 prior to the expiration of a timeout period measured by the step 1522.

When, at the steps 1520 and 1522, it is determined that the network server 114 has not acknowledged the request by the interface station computer 304 in a timely manner, the routine 1406 proceeds to a step 1524, wherein a message is displayed on the display 324 indicating that a transmission failure has occurred.

When, at the steps 1520 and 1522, it is determined that the network server 114 has acknowledged the request by the interface station computer 304 in a timely manner, the routine 1406 proceeds to a step 1528, wherein, in an encrypted format, the information regarding the new Pocket Vault holder is transmitted to the network server 114, along with the interface station operator ID, the interface unit ID, and the Pocket Vault ID.

After the step 1528, the routine 1406 proceeds to steps 1530 and 1532, wherein it is determined whether encrypted validation information (e.g., a PKI certificate) has been received from the network server 114 prior to the expiration of a timeout period measured by the step 1532, and prior to receiving a message from the network server 114 indicating that the request to validate the new Pocket Vault holder has been denied.

When, at the steps 1530 and 1532, it is determined that encrypted validation information has not been received from the network server 114 in a timely manner, or it is determined that a message has been received indicating that the request to validate the new Pocket Vault holder has been denied, the routine 1406 proceeds to a step 1538, wherein a message is displayed on the display 324 indicating that the attempt to validate the Pocket Vault 102 was unsuccessful.

When, at the steps 1530 and 1532, it is determined that encrypted validation information has been received from the network server 114 in a timely manner, the routine 1406 proceeds to a step 1534, wherein the encrypted validation information (e.g., a PKI certificate) from the network server 114 is forwarded to the pocket vault interface unit 302 for forwarding on to the Pocket Vault 102.

After the step 1534, the routine 1406 proceeds to a step 1536, wherein a message is displayed on the display 324 indicating that the attempt to validate the Pocket Vault 102 was successful. In addition to this message, when the pocket vault interface unit 302 forwards this message on to the Pocket Vault 102, the Pocket Vault 102 itself may provide, for example, an audio indication such as a chime, indicating that the Pocket Vault 102 has been successfully validated.

Fig. 16 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO UPDATE INFO ON POCKET VAULT routine of Fig. 14 (step 1410).

As shown, the routine 1410 begins at a step 1602, wherein the Pocket Vault holder is prompted to apply his or her fingerprint to the fingerprint scanner 220 of the Pocket Vault 102, and to interface the Pocket Vault 102 with the pocket vault interface unit 302.

After the step 1602, the routine 1410 proceeds to steps 1604 and 1606, wherein it is determined whether an encrypted message including the ID of the Pocket Vault 102 has been received from the pocket vault interface unit 302 prior to the expiration of a timeout period measured by the step 1606.

When, at the steps 1604 and 1606, it is determined that an encrypted message including the ID of the Pocket Vault 102 has not been received from the pocket vault interface unit 302 in a timely manner, the routine 1410 proceeds to a step 1634, wherein a message is displayed on the display 324 of the interface station computer 304 indicating that the attempt to authorize the Pocket Vault holder was unsuccessful.

When, at the steps 1604 and 1606, it is determined that an encrypted message including the ID of the Pocket Vault 102 has been received from the pocket vault interface unit 302 in a timely manner, the routine 1410 proceeds to a step 1606, wherein the interface station operator is prompted to apply his or her fingerprint to the fingerprint scanner 316 of the pocket vault interface unit 302.

After the step 1606, the routine 1410 proceeds to steps 1608 and 1610, wherein it is determined whether an encrypted message including the ID of the pocket vault interface unit 302 has been received from the pocket vault interface unit 302 prior to the expiration of a timeout period measured by the step 1610.

When, at the steps 1608 and 1610, it is determined that an encrypted message including the ID of the pocket vault interface unit 302 has not been received from the pocket vault interface unit 302 in a timely manner, the routine 1410 proceeds to the step 1634, wherein a message is displayed on the display 324 of the interface station computer 304 indicating that the attempt to authorize the interface station operator was unsuccessful.

After the step 1634, the routine 1410 terminates.

When, at the steps 1608 and 1610, it is determined that an encrypted message including the ID of the pocket vault interface unit 302 has been received from the pocket vault interface unit 302 in a timely manner, the routine 1410 proceeds to a step 1612, wherein the network server 114 is contacted.

After the step 1612, the routine 1410 proceeds to a step 1614, wherein a request to update the information on the Pocket Vault 102 is transmitted to the network server 114.

After the step 1614, the routine 1410 proceeds to steps 1616 and 1618, wherein it is determined whether the network server 114 has acknowledged the request by the interface station computer 304 prior to the expiration of a timeout period measured by the step 1618.

When, at the steps 1616 and 1618, it is determined that the network server 114 has not acknowledged the request by the interface station computer 304 in a timely manner, the routine 1410 proceeds to a step 1620, wherein a message is displayed on the display 324 indicating that a transmission failure has occurred.

When, at the steps 1616 and 1618, it is determined that the network server 114 has acknowledged the request by the interface station computer 304 in a timely manner, the routine 1410 proceeds to a step 1622, wherein, in an encrypted manner, the interface station operator ID, the interface unit ID, and the Pocket Vault ID are transmitted to the network server 114.

After the step 1622, the routine 1410 proceeds to steps 1624 and 1626, wherein it is determined whether encrypted updates have been received from the network server 114 for loading onto the Pocket Vault 102 prior to the expiration of a timeout period measured by the step 1620, and prior to the network server 114 denying the requested attempt to upload information.

When, at the steps 1624 and 1626, it is determined that the encrypted updates have been received in a timely manner, the routine 1410 proceed to a step 1630, wherein the received updates are transmitted to the pocket vault interface unit 302 so that they may be subsequently forwarded to the Pocket Vault 102 for uploading thereto.

After the step 1630, the routine 1410 proceeds to a step 1632, wherein a message is displayed to the holder indicating that the requested updates have been successfully uploaded to the Pocket Vault 102.

After the step 1632, the routine 1410 terminates.

When, at the steps 1624 and 1626, it is determined that the encrypted updates have not been received from the network server 114 in a timely manner, or that the network server 114 has denied the request to upload information onto the Pocket Vault 102, the routine 1410 proceeds to a step 1628, wherein a message is displayed on the display 324 indicating that the attempt to update the information on the Pocket Vault 102 was unsuccessful.

After the step 1628, the routine 1410 terminates.

Fig. 17 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO AUTHORIZE TRANSACTION routine of Fig. 14 (step 1414).

As shown, the routine 1414 begins at a step 1702, wherein the operator of the interface station computer 304 is prompted to input information regarding the proposed transaction involving the Pocket Vault 102.

After the step 1702, the routine 1414 waits at a step 1704 until all of the information regarding the requested transaction has been entered.

After, at the step 1704, it is determined that all of information regarding the requested transaction has been entered, the routine 1414 proceeds to a step 1706, wherein the Pocket Vault holder is prompted to apply his or her fingerprint to the fingerprint scanner 220 of the Pocket Vault 102, and to interface the Pocket Vault with the pocket vault interface unit 302.

After the step 1706, the routine 1414 proceeds to steps 1708 and 1710, wherein it is determined whether an encrypted message including the ID of the Pocket Vault 102 has been received from the pocket vault interface unit 302 prior to the expiration of a timeout period measured by the step 1710.

When, at the steps 1708 and 1710, it is determined that an encrypted message including the ID of the Pocket Vault 102 has not been received from the pocket vault interface unit 302 in a timely manner, the routine 1414 proceeds to a step 1726, wherein a message is displayed on the display 324 of the interface station computer 304 indicating that the attempt to authorize the Pocket Vault holder was unsuccessful.

When, at the steps 1708 and 1710, it is determined that an encrypted message including the ID of the Pocket Vault 102 has been received from the pocket vault interface unit 302 in a timely manner, the routine 1414 proceeds to a step 1712, wherein the interface station operator is prompted to apply his or her fingerprint to the fingerprint scanner 316 of the pocket vault interface unit 302.

After the step 1712, the routine 1414 proceeds to steps 1714 and 1715, wherein it is determined whether an encrypted message including the ID of the pocket vault interface unit 302 has been received from the pocket vault interface unit 302 prior to the expiration of a timeout period measured by the step 1715.

When, at the steps 1714 and 1715, it is determined that an encrypted message including the ID of the pocket vault interface unit 302 has not been received from the pocket vault interface unit 302 in a timely manner, the routine 1414 proceeds to the step 1726, wherein a message is displayed on the display 324 of the interface station

computer 304 indicating that the attempt to authorize the interface station operator was unsuccessful.

After the step 1726, the routine 1414 terminates.

When, at the steps 1714 and 1715, it is determined that an encrypted message including the ID of the pocket vault interface unit 302 has been received from the pocket vault interface unit 302 in a timely manner, the routine 1414 proceeds to a step 1716, wherein the network server 114 is contacted.

After the step 1716, the routine 1414 proceeds to a step 1718, wherein the request regarding the proposed transaction involving the Pocket Vault 102 is transmitted to the network server 114.

After the step 1718, the routine 1414 proceeds to step 1720 and 1722, wherein it is determined whether the transaction request has been acknowledged by the network server 114 before the expiration of a timeout period measured by the step 1722.

When, at the steps 1720 and 1722, it is determined that the request has not been acknowledged in a timely manner, the routine 1414 proceeds to a step 1724, wherein a message is displayed on the display 324 indicating that a transmission failure has occurred.

After the steps 1724, the routine 1414 terminates.

When, at the steps 1722 and 1724, it is determined that the request has been acknowledged in a timely manner, the routine 1414 proceeds to a step 1728, wherein encrypted information about the requested transaction is transmitted to the network server 114, along with the interface station operator ID, the interface unit ID, and the Pocket Vault ID.

After the step 1728, the routine 1414 proceeds to steps 1730 and 1732, wherein it is determined whether an encrypted transaction approval message has been received from the network server 114 prior to the expiration of a timeout period measured by the step 1732.

When, at the steps 1730 and 1732, it is determined that an encrypted transaction approval message has not been received in a timely manner, or that approval for the requested transaction has been denied by the network server 114, the routine 1414 proceeds to a step 1736, wherein a message is displayed on the display 324 indicating that the attempt to authorize the requested transaction has failed.

When , at the steps 1730 and 1732, it is determined that an encrypted transaction approval message has been received in a timely manner, the routine 1414 proceeds to a step 1734, wherein a message is forwarded to the pocket vault interface unit 302 indicating that the requested transaction has been approved. This message may also be used to update information on the Pocket Vault 102, and/or to cause the Pocket Vault 102 to generate an indication (e.g., an audio tone) that the transaction has been approved.

After the step 1734, the routine proceeds to a step 1738, wherein a message is displayed on the display 324 indicating that the requested transaction has been approved.

After the step 1738, the routine 1414 terminates.

Fig. 18 is a flow diagram illustrating an example implementation of the PROCESS UNSUCCESSFUL OPERATOR AUTHENTICATION routine of Fig. 14 (step 1418).

As shown, the routine 1418 begins at a step 1802, wherein the operator of the interface station computer 304 is informed that the attempted use the pocket vault interface unit 302 (when the operator applied his or her finger print to the fingerprint scanner 316) was not authorized.

After the step 1802, the routine 1418 proceeds to a step 1804, wherein the operator is prompted to either: (1) add a NEW OPERATOR to the interface unit 302, or (2) ABORT the attempt to use the interface unit 302.

When, at the step 1806, it is determined that the operator has chosen to ABORT the attempt to use the interface unit 302, the routine 1418 terminates.

When, at the step 1806, it is determined that the operator has chosen to add a NEW OPERATOR, the routine 1418 proceeds to a step 1808, wherein a message is transmitted to the pocket vault interface unit 302 indicating the operator's desire to add a new operator to the pocket vault interface unit 302.

After the step 1808, the routine 1418 proceeds to a step 1810, wherein the operator is prompted to input information regarding the proposed new operator into the interface station computer 304 (e.g., using the user input device 318), and is provided with instructions as to the application of three identical fingerprints from each of his or her two hands to the fingerprint scanner 316 of the interface unit 302.

After the step 1810, the routine 1418 proceeds to a step 1812 wherein the routine 1418 waits until all of the requisite information regarding the proposed new interface station operator has been entered properly.

When, at the step 1812, it is determined that all of the requisite information regarding the proposed new operator has been entered properly, the routine 1418 proceeds to a step 1814, wherein the network server 114 is contacted.

After the step 1814, the routine 1418 proceeds to a step 1816, wherein the request to add the new operator to the pocket vault interface unit 302 is transmitted to the network server 114.

After the step 1816, the routine 1418 proceeds to steps 1818 and 1820, wherein it is determined whether the request by the interface station computer has been acknowledged by the network server 114 prior to the expiration of a timeout period measured by the step 1820.

When, at the steps 1818 and 1820, it is determined that the request has not been acknowledged in a timely manner, the routine 1418 proceeds to the step 1822, wherein a transmission failure message is displayed.

After the step 1822, routine 1418 terminates.

When, at the steps 1818 and 1820, it is determined that the request has been acknowledged in a timely manner, the routine 1418 proceeds to the step 1824, wherein a message, including the information regarding the proposed new operator and the interface unit ID, is transmitted to the network server 114 in an encrypted manner.

After the step 1824, the routine 1418 proceeds to steps 1826 and 1828, wherein it is determined whether encrypted validation information (e.g., a PKI certificate) has been received from the network server 114 prior to the expiration of a timeout period measured by the step 1828, and prior to the network server 114 denying the addition of the new interface station operator.

When, at the steps 1826 and 1828, it is determined that encrypted validation information has been received from the network server 114 in a timely manner, the routine 1418 proceeds to a step 1830, wherein the encrypted validation information (e.g., a PKI certificate) is forwarded from the interface station computer 304 to the pocket vault interface unit 302.

After the step 1830, the routine 1418 proceeds to a step 1834, wherein a message is generated indicating that the attempt to add the new operator to the pocket vault interface unit 302 was successful.

After the step 1834, the routine 1418 terminates.

When, at the steps 1826 and 1828, it is determined that encrypted validation information has not been received from the network server 114 in a timely manner, the routine 1418 proceeds to a step 1832, wherein a message is generated indicating that the attempt to add the new operator to the pocket vault interface unit 302 was unsuccessful.

After the step 1832, routine 1418 terminates.

Fig. 19 is a flow diagram illustrating an example implementation of a primary routine 1900 that may be executed by the network server 114 of Fig. 1.

As shown, the routine 1900 may begin at a step 1902, wherein it is determined whether any requests have been received to register new Pocket Vault holders.

When, at the step 1902, it is determined that a request has been received to register a new Pocket Vault holder, the routine 1900 proceeds to a step 1904, wherein the request to register the new Pocket Vault holder is processed. An example of a routine that may be employed to implement the step 1904 is discussed in more detail below in connection with Fig. 20.

When, at the step 1902, it is determined that no request to register a new Pocket Vault holder has been received, the routine 1900 proceeds to a step 1906, wherein consumer marketing information is compiled and transmitted to subscribing media issuers and advertisers.

After the step 1906, the routine 1900 proceeds to a step 1908, wherein it is determined whether any requests from media issuers or advertisers have been received to update the network server 114.

According to one aspect of the invention, media issuers and advertisers may have the option to utilize the functionality of the network server 114 to update the account characteristics of authenticated Pocket Vault holders. These updates may, for example, be delivered from the computers 108, 110, and 112 to a secure location within the database 406. When each selected holder next synchronizes with network server 114 (e.g., as described below in connection with routine 1914 of Fig. 22), any media characteristics updated by the media issuers or advertisers may be uploaded to that holder's the Pocket Vault 102. The database of account updates may be revised periodically based on the media issuer's systems (e.g., pursuant to the routine 1910 of Fig. 21 - described below). Confirmation of the update process may be provided to the issuer after a synchronization session is complete for a particular Pocket Vault holder (see step 2206 of routine 1914 (Fig. 22) below).

When, at the step 1908, it is determined that a request to update the network server 114 has been received from a media issuer or advertiser, the routine 1900 proceeds to a step 1910, wherein the request from the media issuer or advertiser is processed. An example of a routine that may be employed to implement the step 1910 is discussed in more detail below in connection with Fig. 21.

When, at the step 1908, it is determined that no request from a media issuer or advertiser to update the network server 114 has been received, the routine 1900 proceeds to a step 1912, wherein it is determined whether any requests have been received from holders to update information on their Pocket Vaults.

When, at the step 1912, it is determined that such a request has been received, the routine 1900 proceeds to a step 1914, wherein the request to update the Pocket Vault information is processed. An example of a routine that may be employed to implement the step 1914 is described in more detail below in connection with Fig. 22.

When, at the step 1912, it is determined that no request from a holder to update information on a Pocket Vault 102 has been received, the routine 1900 proceeds to a step 1916, wherein it is determined whether any holders have requested that new files be loaded onto the network server 114.

When, at the step 1916, it is determined that a holder has requested that a new file be loaded onto the network server 114, the routine 1900 proceeds to a step 1918, wherein the holder's request to load the new file onto the network server 114 is processed. An example of a routine that may be employed to implement the step 1918 is described in more detail below in connection with Fig. 23.

When, at the step 1916, it is determined that no request by a holder to load a file onto the network server 114 has been received, the routine 1900 proceeds to a step 1920, wherein it is determined whether any requests have been made to authorize transactions. Such a request may be made, for example, by a merchant operating a commercial interface station 104c. In this regard, it should be appreciated that, when a token 102a is employed to engage in a transaction with a commercial card reader 106 or a commercial bar code reader 107, a request for transaction approval may not be made to the network server 114. Instead such a transaction approval request may be made through conventional, existing communication and approval channels for such devices. Therefore, it should be understood that the step 1922 is generally reached only when it is possible for the network server 114 to check the identity of the Pocket Vault holder, the

identity of the Pocket Vault 102, and possibly identity of the operator of a commercial interface station, based on communications with the Pocket Vault 102 (e.g., via a commercial interface station 104c or via a wireless network such as Bluetooth).

When, at the step 1920, it is determined that a request to authorize a transaction has been made, routine 1900 proceeds to a step 1922, wherein the request to authorize the transaction is processed. An example of a routine that may be employed to implement the step 1922 is discussed in more detail below in connection with Fig. 24.

When, at the step 1920, it is determined no request to authorize a transaction has been made, the routine 1900 returns to the step 1902 (discussed above). With regard to the routine 1900 of Fig. 19, it should be appreciated that all of the requests to accomplish the various tasks may be placed in a queue so that they are serviced on a first-come, first-served or any other basis, rather than servicing them in the particular order shown in Fig. 19.

Fig. 20 is a flow-diagram illustrating an example of a routine that may be employed to implement the step 1904 of the routine 1900 (Fig. 1).

As shown, the routine 1904 begins at a step 2002, wherein a request received from the interface station computer 304 to register a new Pocket Vault holder is acknowledged, and the network server 114 requests the interface station computer 304 to transfer the relevant information regarding the proposed new holder to the network server 114.

After the step 2002, the routine 1904 proceeds to a step 2004, wherein the routine 1904 waits for all of the requisite holder registration information to be received from the interface station computer 304.

When, at the step 2004, it is determined that all of the requisite holder registration information has been received from the interface station computer 304, the routine 1904 proceeds to a step 2006, wherein it is determined whether the proposed Pocket Vault use is authorized. An example of a routine that may be employed to implement the step 2006 is discussed below in connection with Fig. 25. In determining whether a particular Pocket Vault use is authorized, there are numerous parameters which may be checked. For example, the port to which the interface station computer is connected (e.g., the telephone number or IP address of the computer) may be checked to ensure that it is authorized. Additionally, information from the interface station computer 304 (e.g., a "cookie") may be checked to ensure that the computer itself has been registered with the

system. Further, it can be checked whether the current operator of the interface station computer 304 is registered as being associated with the interface station computer 304 being used, and that the proposed new Pocket Vault holder is authorized to use that particular the Pocket Vault 102. In sum, the identity of (1) each piece of equipment, (2) each operator of each piece of equipment, and (3) each location of each piece of equipment may be checked to ensure that the particular use of the Pocket Vault is authorized. It should be appreciated fewer than all of these parameters, different parameters, and/or additional parameters can be checked in alternative embodiments of the invention, and that the invention is not limited to embodiments wherein all of the aforementioned parameters are checked to verify that a particular Pocket Vault use is authorized.

When, at the step 2006, it is determined that the Pocket Vault use is not authorized, the routine 1904 terminates. In such a situation, it is also possible to generate some sort of security alert message to put someone or some entity on notice that an unauthorized use of a Pocket Vault has occurred.

When, the routine 2006 has determined that the proposed Pocket Vault use is authorized, the routine 1904 proceeds to a step 2008, wherein all of the relevant information regarding the new Pocket Vault registration is logged into the database 406 of the network server 114 (Fig. 4). As shown in Fig. 20, this information may include, for example, the interface station operator ID, the interface unit ID, the Pocket Vault ID, and all of the relevant information relating to the new Pocket Vault holder.

After the step 2008, the routine 1904 proceeds to a step 2010, wherein the network server 114 transmits encrypted validation information to the interface station computer 304, which then may be passed on to the pocket vault interface unit 302, and then to the Pocket Vault 102, so as to enable the new holder's fingerprint to be stored in the memory of the Pocket Vault 102.

After the step 2010, the routine 1904 terminates.

Fig. 21 is a flow diagram illustrating example of a routine that may be employed to implement the step 1910 of the primary routine 1900 (Fig. 19).

As shown, the routine 1910 begins at a step 2102, wherein it is determined whether all of the requested updates have been received from the media issuer or advertiser.

When, at the step 2102, it has been determined that all of the requested updates have been received, the routine 1910 proceeds to a step 2104, wherein it is determined whether the media issuer or advertiser is authorized access to the network server 114. This authorization process may require some sort of authentication of the identity of the computer used by the media issuer or advertiser requesting the update, the operator of the computer, and/or the location of the computer, in a manner similar to that in which the interface stations 104 and their operators are authorized.

When, at the step 2104, it is determined that the media issuer or advertiser is not authorized access to the network server 114, the routine 1900 proceeds to a step 2106, wherein a message is transmitted to the media issuer or advertiser informing the media issuer or advertiser that access to the network server 114 has been denied.

After the step 2106, the routine 1910 terminates.

When, at the step 2104, it is determined that the media issuer or advertiser is authorized access to the network server 114, the routine 1910 proceeds to a step 2108, wherein the updates received from the media issuer or advertiser are logged onto the network server 114.

After the step 2108, the routine 1910 terminates.

Fig. 22 is a flow diagram illustrating an example a routine that may be employed to implement the step 1914 of the primary routine 1900 (Fig. 19).

As shown, the routine 1914 begins at the step 2006 (discussed below in connection with Fig. 25), wherein it is determined whether the attempted Pocket Vault use is authorized.

When, at the step 2006, it is determined that the Pocket Vault use is not authorized, the routine 1914 terminates.

When, at the step 2006, it is determined that the Pocket Vault use is authorized, the routine 1914 proceeds to a step 2202, wherein encrypted updates are transmitted to the interface station computer 304 for loading onto the Pocket Vault 102.

After the step 2202, the routine 1914 proceeds to steps 2204 and 2206, wherein the time and date of the updates are logged (step 2204), and the media issuers or advertisers are informed that the updates have been made (step 2206).

Fig. 23 is a flow diagram illustrating an example of a routine that may be employed to implement the step 1918 of the primary routine 1900 (Fig. 9).

As shown, the routine 1918 begins at a step 2302, wherein it is determined whether the file to be loaded onto the network server 114 relates to a secure media issuer.

When, at the step 2302, it is determined that the file does not relate to a secure media issuer, the routine 1918 proceeds to a step 2304, wherein the network server 114 is updated with the non-secure file.

After the step 2304, the routine 1918 terminates.

When, at the step 2302, it is determined that the to-be-loaded file does relate to a secure media issuer, the routine 1918 proceeds to a step 2306, wherein it is determined whether the secure media issuer is a Pocket Vault participant (i.e., a media issuer having access to the network server 114).

When, at the step 2306, it is determined that the secure media issuer is not a Pocket Vault participant, the routine 1918 proceeds to a step 2308, wherein an advisory is sent to the holder indicating an inability to load the file, and inquiring as to whether the holder desires to load the file in a non-secure format. The holder may, for example, opt to load the file to the network server 114 in such a way that the content of the file is not encodable to the Chameleon Card, but can be displayed and shown to a POS operator and manually keyed in at POS by the POS operator.

After the step 2308, the routine 1918 proceeds to a step 2316, wherein it is determine whether the holder has elected to load the file in a non-secure format.

When, at the step 2316, it is determined that the holder has elected not to load the file in a non-secure format, the routine 1918 terminates.

When, at the step 2316, it is determined that the holder has elected to load the file in a non-secure format, the routine 1918 proceeds to a step 2318, wherein the file is loaded onto the network server 114 in a non-secure format.

After the step 2318, the routine 1918 terminates.

When, at the step 2306, it is determined that the secure media issuer is a Pocket Vault participant, the routine 1918 proceeds to a step 2310, wherein the media issuer is queried as to the account status of the holder.

After the step 2310, the routine 1918 proceeds to a step 2312, wherein it is determined whether authorization has been received from the media issuer to load the file.

When, at the step 2312, it is determined that authorization has not been received from the media issuer, the routine 1918 proceeds to the step 2308 (discussed above).

When, at the step 2312, it is determined that authorization has been received from the media issuer, the routine 1918 proceeds to a step 2314, wherein the network server 114 is updated with the secure file.

After the step 2314, the routine 1918 terminates.

Fig. 24 is a flow diagram illustrating an example of a routine that may be employed to implement the step 1922 of the primary routine 1900 (Fig. 19).

As shown, the routine 1922 begins at the step 2006 (discussed below in connection with Fig. 25), wherein it is determined whether the attempted use of the Pocket Vault 102 is authorized.

When, at the step 2006, it is determined that the attempted Pocket Vault use is not authorized, the routine 1922 terminates.

When , at the step 2006, it is determined that the attempted Pocket Vault used is authorized, the routine 1922 proceeds to a step 2402, wherein it is determined whether the requested transaction is within acceptable account parameters (e.g., as set by the media issuer).

When, at the step 2402, it is determined that the requested transaction is not within acceptable account parameters, the routine 1922 proceeds to a step 2404, wherein a message is transmitted to the entity that requested the transaction (e.g., a commercial interface station 104C, a card reader 106, or a barcode reader 107) indicating that the transaction is outside of acceptable account parameters.

After the step 2404, the routine 1922 terminates.

When, at the step 2402, it is determined that the requested transaction is within acceptable account parameters, information regarding the transaction is logged into the database 406 of the network server 114 (Fig. 4). As shown, the logged information may include the identification of the entity with which the transaction took place, the Pocket Vault ID (if available), and the time and date of the transaction.

After the step 2406, the routine 1922 proceeds to a step 2408, wherein an encrypted approval message is transmitted to the entity with which the transaction is being attempted (e.g., a commercial interface station 104C, a card reader 106, or a barcode reader 107).

After the step 2408, the routine 1922 terminates.

Fig. 25 is a flow diagram illustrating an example of a routine that may employed to implement the step 2006 of the routines 1904 (Fig. 20), 1914 (Fig. 22), and 1922 (Fig. 24).

As shown, the routine 2006 begins at a step 2502, wherein it is determined whether the point of sale terminal or other entity with which a transaction is being attempted is connected to a valid source (e.g., an authorized telephone line or an authorized internet protocol (IP) address).

When, at the step 2502, it is determined that the entity proposing the transaction is not connected to a valid source, the routine 2006 proceeds to a step 2510, wherein the transaction is refused, and a security alert is generated so that appropriate action(s) may be taken.

When, at the step 2502, it is determined that the entity proposing the transaction is connected to a valid source, the routine 2006 proceeds to a step 2504, wherein it is determined whether the ID of the interface station, card reader, barcode reader or RFID interrogator is valid, and is properly linked to the source to which is connected.

When, at the step 2504, it is determined that the ID of the entity proposing the transaction is not valid, the routine proceeds to the step 2510 (discussed above).

When, at the step 2504, it is determined that the ID of the entity proposing the transaction is valid, the routine 2006 proceeds to a step 2506, wherein it is determined whether the Pocket Vault ID (if available) is valid. It should be appreciated that, when a card reader 106, a barcode reader 107, an RF signal receiver, or an RFID interrogator is employed, it is possible that the ID from the Pocket Vault will not be transmitted to the network server 114. Therefore, the step 2506 may be skipped in such a situation.

When, at the step 2506, it is determined that the Pocket Vault ID (when available and required) is not valid, the routine 2006 proceeds to the step 2510 (discussed above).

When, at the step 2506, it is determined that the Pocket Vault ID (when) is valid or is not required, the routine 2006 proceeds to a step 2508, wherein it is determined whether the Pocket Vault ID (if available) is linked to the ID of the entity proposing the transaction, e.g., a commercial interface station 104c, a card reader 106, a barcode reader 107, or an RFID interrogator 107.

When, at the step 2508, it is determined that the ID of the Pocket Vault 102 (when available) is not linked to the ID of the entity proposing the transaction, the routine 2006 proceeds to the step 2510 (discussed above).

When, at the step 2508, it is determined that the Pocket Vault ID is linked to the ID of the entity proposing the transaction, or that the ID of the Pocket Vault is not required, the routine 2006 proceeds to a step 2512, wherein the Pocket Vault use is authorized.

With regard to the information checked in connection with the routine 2006 to determine whether a particular Pocket Vault use is authorized, it should be appreciated that, in some embodiments, fewer than all of the verification steps discussed above may be performed when lesser degrees of security are desired or required. For example, in some embodiments, there may be no restrictions as to who can operate an interface station, the source to which the station is connected, and/or the ID of the station.

Figure 27 illustrates a network system similar to that described hereinabove. The system of Fig. 27, however, includes several additional components which serve to increase the network's functionality and utility. Accordingly, it should be appreciated that, in addition to the components illustrated in Fig. 27, the system may also include all or some of the components and features of the system described above in connection with Figs. 1-26, and may also incorporate all or some of that system's functionality.

As shown in Fig. 27, the Pocket Vault 102 may be coupled to an interface station 104 (including an interface unit 302 coupled to an the interface station computer 304). The interface unit 302 may include a communication port 2706, which is adapted to perform basic communications functions for interaction between the interface unit 302 and each of the Pocket Vault 102 and the interface station computer 304. This communication can take place over physical wires using a USB protocol or HotWire, or any other suitable protocol. Alternatively, the communication can be wireless, using a standard wireless protocol, such as Bluetooth, or any other suitable protocol. The communication port 2706 may, of course, be adapted to perform communications functions depending on the requirements on the particular protocol used. In an example embodiment, a USB protocol is used, and the interface unit 302 is connected to the interface station computer 304 through a USB port. Several suitable methods/techniques for interfacing the Pocket Vault 102 with the interface unit 302 are described above.

In addition to the communication port 2706, as in the embodiment described above, the interface unit 302 contains a stripe reader 315. The purpose and operation of the stripe reader 315 is described below in connection with Figure 34.

The interface station computer 304 may be any suitable computer that employs one or more processors to execute instructions stored in memory. The interface station computer 304 may even comprise several inter-networked computers.

In the illustrative embodiment shown, the interface station computer 304 may use the communication software 2710 to communicate with the network server 114 via the network 2724. The communication software 2710 may be any of a number of communication programs known in the art, and the invention is not limited to any particular type of software. The software 2710 may, for example, comprise a web browser, a terminal emulation program, a proprietary program, or any other software module capable of communicating with other computers using the network 2724. The network 2724 may be any communication network known in the art. For example, the network 2724 may comprise the World Wide Web, a Local Area Network, or any other networking arrangement adapted for communication between digital computers.

In the embodiment shown, the communication software 2710 uses internet settings 2722 when accessing the network 2724. The internet settings 2710 may include any user preferences or software settings relevant to communication functions and usability of the communication software 2710. The internet settings 2722 may comprise, for example, the network name and the identification of the interface station computer 304, an identification of communications protocols used to connect to the network 2724, network preferences, such as whether any proxy servers may or should be used, a list of frequently-used servers, cookies previously obtained from various websites, digital certificates, personal bookmarks, user identity data, user password data for various servers, etc.

The communication software 2710 may access the network 2724 through communication protocol layer 2714. Depending on how the interface station computer 304 is physically connected to the network 2724. The communication protocol layer 2714 may be dial-up software, a TCP/IP layer, or any other suitable networking layer. The communication protocol layer 2714 may, for example, execute low-level communication functions, thereby providing useful abstractions to the communication software 2710. In an example embodiment, the interface station computer 304 is connected to the network 2724 using a modem, and the communication protocol layer 2714 is a dialup software module.

As shown, the interface station computer 304 may also contain one or more communication drivers 2712. Although multiple drivers may, in fact, be employed, for simplicity of discussion, the description hereinafter may refer to all such drivers as a single "driver." The communication driver 2712 acts both as a device driver for the interface unit 302, and also as a communications driver capable of accessing internet settings 2722 and facilitating communications between the Pocket Vault 102 and the server 114 by using the communication protocol layer 2714 to establish a connection to the network server 114 through the network 2724.

The network server 114 may comprise any suitable processor-based device or its equivalent. It may be either a single or multi-processor machine, or even a collection of servers inter-networked together. In one embodiment, the network server 114 stores both data and applications that are accessible to users. The network server 114 may, for example, store and serve a website, i.e., a collection of web pages and data that are available to users via a browser.

The network server 114 may include one or more controllers 402 and a database 406, as described above in connection with Figure 4. In addition, the network server 114 may include a communication protocol layer 2716, which provides low-level communication functions to server communications software. The communication protocol layer 2716 may be, but need not be, the same as the communication protocol layer 2714 of the interface station computer 304.

As shown in Fig. 27, the network server 114 may communicate through the network 2724 with an issuer authority 2718. The issuer authority 2718 may correspond, for example, to any of the advertiser(s) 108, non-financial media issuer(s) 110, or financial media issuer(s) 112 described above in connection with Fig. 1, or may be any entity designated to represent any of the same.

Overall, the networking arrangement illustrated in Fig. 27 allows the Pocket Vault 102 to access the network server 114. It also allows the interface station computer 304 to access restricted portions of the network server 114, such as, for example, user data stored in the database 406, when access is authenticated through communication from the Pocket Vault 102 to the network server 114. Authentication and access to restricted areas of the network server 114 will be further described below.

In order for the Pocket Vault 102 to perform communications functions, as well as other functions described elsewhere herein, the Pocket Vault 102 may be driven by

control software 2708. Fig. 28 is a block diagram illustrating example components of the control software 2708 that may be disposed on the Pocket Vault 102.

As shown, the control software 2708 may include components such as a communications software module 2802, a card loading module 2804, an RFID tag loading module 2805, an internet settings management module 2806, a synchronization module 2808, a statistics module 2810, and a security module 2812. It should be appreciated, of course, that the control software 2708 is not limited to the illustrative modules shown, and that the control software 2708 may comprise fewer modules or additional modules to perform other functions, such as the functionality described above in connection with Figs. 7-12.

The communications software module 2802 may, for example, be responsible for communications with the network server 114 and with the interface station computer 304, in the manner discussed below.

The card loading module 2804 may, for example, be responsible for loading data for new cards or tokens and storing such data in memory, as well as for transferring this data to the network server 114, when appropriate. Examples of how card/token data may be loaded onto the Pocket Vault 102 are discussed below in connection with Fig. 34.

The RFID tag loading module 2805 may, for example, be responsible for loading data for new RFID tags and storing such data in memory, as well as for transferring this data to the network server 114, when appropriate. Examples of how RFID tag data may be loaded onto the Pocket Vault 102 are discussed below in connection with Fig. 40.

Internet settings management module 2806 may, for example, be responsible for managing the storage and use of internet settings by the Pocket Vault 102. Such internet settings may, for example, correspond to any of the internet settings 2722 that may be stored on the interface station computer 304. The internet settings management module 2806 may allow a user to store, manage, and transfer internet settings, e.g., cookies and preference settings, from one computer to another. Operation of the internet settings management module 2708 will be further described below in connection with the steps 3310 and 3320 of the routine 3024 (Fig. 33).

The synchronization module 2808 may, for example, be responsible for synchronizing data and settings stored on the Pocket Vault 102 with data and settings stored on the network server 114. Operation of the synchronization module 2808 is described below in connection with Fig. 35.

The statistics module 2810 may, for example, collect statistics concerning use of the Pocket Vault 102. Such statistics may, for example, include information such as the number of accesses to various cards stored in the memory of the Pocket Vault 102, the number of financial transactions engaged in, the date of the last update of the Pocket Vault 102, the total amount and kind of data transferred between the Pocket Vault 102 and each interface station 104 and/or the network server 114. In addition, the statistics module 2810 may be adapted to be customized by the user.

The security module 2812 may, for example, ensure security of authentication and communications. All communications to and from the network server 114 and the interface station 104 may be encrypted by the security module 2812, so that any attacker who intercepts those communications will receive no useful information.

Any of numerous types of encryption may be used to satisfactorily protect communications between the Pocket Vault 102 and the other devices in the network. For example, one of the asymmetric-key encryption types, such as public key encryption or private key encryption, may be used. These public/private encryption techniques are well known in the art and therefore will not be described here in detail. Alternatively, one-time pad encryption or other encryption techniques may be used to achieve a similar objective.

As discussed above, the Pocket Vault 102 may be adapted to not release any personal or secure information, even encrypted, until the holder presents satisfactory verification of his or her identity, such as, for example, presenting the holder's fingerprint to the fingerprint scanner 220 or entering a password. In addition, fingerprint and password protection may be used together for authentication purposes, such that personal or secure information can be transferred or released only if the holder has been successfully authenticated using both techniques.

In alternative embodiments, security may be implemented using different measures, or may be omitted altogether in situations where the interface station computer 304 is a trusted host. In addition, security module 2812 may be called on to perform security functions in situations other than communicating with the network server 114 and the interface station computer 304.

The manner of communication among the Pocket Vault 102, the network server 114, and an interface station computer 304 will now be described in connection with Figure 29. Figure 29 is a data flow diagram illustrating how data may be transferred

between the Pocket Vault 102 and a user interface 2902 of the interface station computer 304. The user interface 2902 may, for example, comprise a web browser included in the communications software 2710 running on the interface station computer 304. Alternatively, it may be a stand-alone application that allows a user to interact with the communications software 2710 and, through it, interact with a website located on the network server 114.

In the illustrative embodiment shown, the data transfer takes place via the communication driver 2712, the network server 114, and the communications software 2710, data can flow in both directions at all connection points, and all communications between the Pocket Vault 102 and the user interface 2902 of the interface station computer 304 pass through the network server 114.

Using the arrangement shown, the user may, for example, update settings on the Pocket Vault 102 by using the user interface 2902 and the communication software 2710 to update settings on the network server 114, and then instructing the network server 114 to update settings on the Pocket Vault 102 via the communication driver 2712.

In one embodiment, the network server 114 implements a website, where user information may be selectively stored and accessed by a person using the communication software 2710 (e.g., a web browser) running on the interface station computer 304, and any user may access the website on the network server 114. However, the website may have a so-called "restricted area" which can be accessed only after the user has authenticated his or her identity. As used herein, the term "restricted area" or "restricted information" means any data that is not available to general public without some sort of authentication. For example, each user may have preferences stored in the database 406 that would indicate how the main site should be presented to that user. Those preferences will not be available to other users. In addition to such relatively low-security settings, such as website preferences, database 406 may also contain private user information, such as information about a user's credit cards and identity information. Access to this restricted information may be limited, for example, to only "authenticated" users.

Authentication of a Pocket Vault holder may be achieved, for example, by the holder applying a fingerprint to the fingerprint scanner 220 of the Pocket Vault 102, interfacing the Pocket Vault 102 with the interface unit 302 (which acts essentially as a pass-through device), and establishing a connection between the Pocket Vault 102 and

the network server 114 via the communication driver 2712. Based on communications with the Pocket Vault 102 via this "connection," the website may determine: (1) whether the Pocket Vault 102 has been "validated," i.e., whether a fingerprint has been stored in the fingerprint memory of the Pocket Vault 102 and whether validation information (e.g., a PKI certificate) is present on the Pocket Vault 102, and (2) whether the Pocket Vault 102 has been authenticated, i.e., whether the fingerprint recently scanned by the Pocket Vault 102 matched the fingerprint stored in the fingerprint memory of the Pocket Vault 102. If the website determines that the Pocket Vault 102 has not yet been validated, the user may be given an option to validate the Pocket Vault 102 using the website software. If the website determines that the Pocket Vault 102 has been validated and authenticated, then the network server 114 may enable the authenticated holder to access or perform functions relating to some or all of the restricted area of the database 406 containing that holder's information.

Communication driver 2712 may be a light-weight application that can access and modify the internet settings 2722, and can also access communications protocol layer 2714, but cannot transfer information to any other software programs. For example, the communication driver 2712 may access the internet settings 2722 in order to determine that the interface station computer 304 is connected to the network 2724 through a dial-up connection; following that, it may initiate the dial-up connection or use an established connection through the communications protocol layer 2714 in order to tunnel packets from the Pocket Vault 102 to the network 2724.

Fig. 30 is a flow diagram illustrating an example implementation of the PROCESS REQUEST TO ACCESS WEBSITE routine 1422 shown in Fig. 14, which may be executed by the controller 308 of the interface station computer 304. As discussed above in connection with Fig. 14, it should be appreciated that this routine need not be accessed as a result of a user selecting it from the menu displayed in the step 1402. Rather, a user may simply use a browser to directly log onto the website on the network server 114.

As shown, the routine 1422 begins at a step 3002, wherein the interface station computer 304 is caused to access the website on the network server 114, e.g., by using a browser to access the website.

After the step 3002, the routine 1422 proceeds to a step 3004, wherein it is determined whether the requisite communication drivers 2712 have been installed.

When, at the step 3004, it is determined that the requisite communication drivers 2712 have not been installed, the routine 1422 proceeds to an INSTALL DRIVER(S) routine 3006 (discussed below in connection with Fig. 31), which is responsible for installing the communication drivers 2712.

After the routine 3006 has completed, the routine 1422 proceeds to a step 3008, wherein the communication drivers 2712 are caused to become operational.

When, at the step 3004, it is determined that the requisite drivers 2712 have already been installed, the routine 1422 proceeds directly to the step 3008 (discussed above).

After the step 3008, the routine 1422 proceeds to steps 3010-3016, wherein attempts are made to establish a connection between the Pocket Vault 102 and the website on the network server 114 within a time out period determined by the step 3014. Each time it is determined that the connection has not yet been established, the user is prompted to interface the Pocket Vault 102 with the interface unit 302 and to connect the interface unit 302 to the interface station computer 304 (e.g., using a USB cable).

When, during the steps 3010-3016, it is determined that a connection has not been established between the Pocket Vault 102 and the website in a timely manner, the routine 1422 proceeds to a step 3026, wherein a message is displayed to the user regarding the unsuccessful communication attempt between the Pocket Vault 102 and the website on the network server 114.

After the step 3026, the routine 1422 terminates.

When, during the steps 3010-3016, it is determined that a connection has been successfully established between the Pocket Vault 102 and the website on the network server 114, the routine 1422 proceeds to a step 3018, wherein it is determined whether the Pocket Vault 102 has been validated, e.g., whether a holder's fingerprints and a PKI certificate are stored therein. The website may, for example, make this determination based upon the messages exchanged during the handshaking protocol engaged in between the Pocket Vault 102 and the network server 114.

When, at the step 3018, it is determined that the Pocket Vault 102 has not yet been validated, the routine 1422 proceeds to a NEW POCKET VAULT HOLDER routine 3020, which is discussed below in connection with Fig. 32.

When, at the step 3018, it is determined that the Pocket Vault 102 has already been validated, the routine 1422 proceeds to an EXISTING POCKET VAULT HOLDER routine 3024, which is discussed below in connection with Fig. 33.

After completion of the EXISTING POCKET VAULT HOLDER routine 3024, the routine 1422 terminates.

After completion of the NEW POCKET VAULT HOLDER routine 3020, the routine 1422 proceeds to a step 3022, wherein it is determined whether a new holder was successfully validated.

When, at the step 3022, it is determined that a new holder was successfully validated, the routine 1422 proceeds to the EXISTING POCKET VAULT HOLDER routine 3024 (discussed above).

When, at the step 3022, it is determined that a new holder was not successfully validated, the routine 1422 terminates.

Fig. 31 is a flow diagram illustrating an example implementation of the INSTALL DRIVER(S) routine 3006 shown in Fig. 30.

As shown, the routine 3006 begins at a step 3102, wherein the necessary communication drivers 2712 are downloaded from another computer, e.g., a website on the World Wide Web.

After the step 3102, the routine 3006 proceeds to steps 3104-3108, wherein the necessary communication drivers 2712 are installed on the interface station computer 304 and registered with network server 114, and the preferences for the communication drivers 2712 are set either automatically or in response to user input. During the step 3106, the communication driver 2712 may communicate with the network server 114 in order to register itself and its attributes. Among these attributes can be such things as a unique identifier for the interface station computer 304 on which that driver is installed, the identity of the user registering it, and other such items. The preferences that may be set by the user during the step 3108 may, for example, include information such as how and where to access the internet settings 2722, how many attempts at connection should be performed, etc.

After the step 3108, the routine 3006 terminates.

Fig. 32 is a flow diagram illustrating an example implementation of the NEW POCKET VAULT HOLDER routine 3020 shown in Fig. 30.

As shown, the routine 3020 begins at a step 3202, wherein it is determined whether the new holder has indicated that he or she has already established an account with the website on the network server 114.

When, at the step 3202, it is determined that the new holder has not indicated the existence of a previously-established account, the routine 3020 proceeds to a step 3204, wherein a new account is established on the website on the network server 114 in response to user input to a browser running on the interface station computer 304.

After the step 3204, the routine 3020 proceeds to a step 3206, wherein the new holder is prompted to apply his or her fingerprint to the fingerprint scanner 220 while the Pocket Vault 102 is interfaced with the interface unit 302. The user is further prompted to follow the directions on the Pocket Vault 102. As discussed above in connection with Figs. 7 and 8, when a fingerprint is applied to a fingerprint scanner 220 of an un-validated device, the user is instructed by the Pocket Vault to apply six finger prints (three from one finger on the left hand and three from one finger on the right hand) sequentially to the fingerprint scanner 220, waiting for a beep each time. As discussed in connection with Fig. 8, after the new holder has completed this task, an encrypted message including the Pocket Vault ID may be released from the Pocket Vault to the interface unit 302. Because of the established connection between the Pocket Vault 102 and the website on the network server 114, this encrypted message should reach the website. And, in response to receiving this encrypted message, the website should release encrypted validation information (e.g., a PKI certificate) back to the Pocket Vault 102 via the established connection.

After the step 3206, the routine 3020 proceeds to steps 3208-3210, wherein it is determined whether the Pocket Vault 102 has released the encrypted message including the Pocket Vault ID to the website before a timeout period has elapsed.

When, at the step 3210, it is determined that the timeout period elapsed before the encrypted message including the Pocket Vault ID was released to the website, the routine 3020 proceeds to a step 3220, wherein a message is displayed to the user concerning the unsuccessful attempt to validate the Pocket Vault holder.

After the step 3220, the routine 3020 terminates.

When, at the steps 3208-3210, it is determined the Pocket Vault 102 has released the encrypted message including the Pocket Vault ID to the website before the timeout period elapsed, the routine 3020 proceeds to a step 3212, wherein it is determined

whether the website has released the encrypted validation information (e.g., a PKI Certificate) to the Pocket Vault 102.

When, at the step 3210, it is determined that the timeout period elapsed before the website released the encrypted validation information (e.g., a PKI Certificate) to the Pocket Vault 102, the routine 3020 proceeds to the step 3220 (discussed above).

When, at the step 3210, it is determined that the website released the encrypted validation information (e.g., a PKI Certificate) to the Pocket Vault 102 before the timeout period elapsed, the routine 3020 proceeds to a step 3216, wherein a message is displayed to the user concerning the successful validation of the new Pocket Vault holder.

After the step 3216, the routine 3020 terminates.

When, at the step 3202, it is determined that the new holder has indicated the existence of a previously-established account, the routine 3020 proceeds to a step 3218, wherein a check is made to verify the holder's identity. The holder may, for example, be required to enter personal information, such as name, contact information, and security information to verify his or her identity.

When, at the step 3218, it is determined that the holder has successfully verified his or her identity, the routine 3020 proceeds to the step 3206 (discussed above), with the holder's previously-stored account information being used for the new Pocket Vault 102.

When, at the step 3218, it is determined that the holder has not successfully verified his or her identity, the routine 3020 proceeds to the step 3220 (discussed above).

Fig. 33 is a flow diagram illustrating an example implementation of the EXISTING POCKET VAULT HOLDER routine 3024 shown in Fig. 30.

As shown, the routine 3024 begins at a step 3302, wherein it is determined whether the Pocket Vault 102 has been authenticated, e.g., whether the Pocket Vault 102 has determined that a fingerprint applied to the fingerprint scanner 220 matches one of the fingerprints stored in the fingerprint memory of the Pocket Vault 102. This authentication procedure may operate as described above in connection with the step 712 (Fig. 7), or an additional or different routine may be employed (e.g., as part of the security module 2812 described above in connection with Fig. 28) to determine whether the holder has successfully authenticated his or her identity, thereby enabling the network server 114 to establish a "trust" relationship with the Pocket Vault 102.

When, at the step 3302, it is determined that the Pocket Vault 102 has not been properly authenticated, the routine 3024 proceeds to a step 3304, wherein the holder is prompted to apply his or her fingerprint to the fingerprint scanner 220 of the Pocket Vault 102 while the Pocket Vault 102 is interfaced with the interface unit 302, i.e., while keeping the connection established between the Pocket Vault 102 and the website on the network server 114.

As shown, the step 3306 determines whether the Pocket Vault 102 has been properly authenticated prior to the expiration of a timeout period.

When, at the step 3306, it is determined that the timeout period elapsed before the Pocket Vault 102 was authenticated, the routine 3024 proceeds to a step 3308, wherein a message is displayed indicating that the authentication attempt was unsuccessful.

After the step 3308, the routine 3024 terminates.

When, at the step 3302, it is determined that the Pocket Vault 102 has been properly authenticated, the routine 3024 proceeds to a step 3310, wherein the communication driver 2712 causes the internet settings 2722 of the interface station computer 304 to be adjusted to reflect certain internet settings stored in the Pocket Vault 102, e.g., by the internet settings management module 2806. In this manner, the internet settings of the Pocket Vault 102 may be "ported" to the interface station computer 304 so that the browser operating on the interface station computer 304 may take advantage of those settings while the Pocket Vault 102 is connected to the website on the network server 114 via the communication driver 2712. The internet settings of the Pocket Vault 102 that may be ported to the interface station computer 304 in this manner may comprise, for example, the network name and identification of the Pocket Vault 102, an identification of communications protocols used to connect to the network 2724, network preferences, such as whether any proxy servers may or should be used, a list of frequently-used servers, cookies previously obtained from various websites, digital certificates, personal bookmarks, user identity data, user password data for various servers, etc.

The internet settings on the Pocket Vault 102, and porting of the same to the interface station computer 304, may be managed, for example, by one or more modules of the control software, e.g., the internet settings management module 2806. In one embodiment, the user may elect which internet settings are to be ported to the interface

station computer 304 during the step 3310. This functionality may be accomplished, for example, during a SET PREFERENCES routine 3324 (described below in connection with Fig. 39).

After the step 3310, the routine 3024 proceeds to a step 3312, wherein it is determined whether one of several "functions" has been selected. In the illustrative embodiment shown, the seven available functions are: (1) CARD LOADING (see CARD LOADING routine 3314 -- discussed below in connection with Fig. 34), (2) RFID TAG LOADING routine 3315 – discussed below in connection with Fig. 40, (3) SYNCHRONIZATION (see SYNCHRONIZATION routine 3316 -- discussed below in connection with Fig. 35), (4) RECOVERY (see RECOVERY routine 3318 -- discussed below in connection with Fig. 36), (5) IDENTITY PORTING OPTIONS (see IDENTITY PORTING OPTIONS routine 3320 -- discussed below in connection with Fig. 337), (6) BACKUP (see BACKUP routine 3322 -- discussed below in connection with Fig. 38), (7) SET PREFERENCES (see SET PREFERENCES routine 3324 -- discussed below in connection with Fig. 39), AND (8) TERMINATE SESSION (see step 3326). It should be appreciated that the invention is not limited to the specific functions shown, and that additional, different or fewer functions may be employed.

It should further be appreciated that some or all of the illustrated functions, or operations relating to such functions, may be initiated automatically or may require user initiation, depending on the setting of preferences. For example, the SYNCHRONIZATION routine 3316 may be initiated automatically after completion of the step 3310, if preferences so indicate. Alternatively, certain steps required to accomplish synchronization of the Pocket Vault 102 and the website on the network server 114 may be taken, without actually completing the synchronization. For example, the synchronization module 2808 of the control software 2708 may automatically initiate a comparison of the contents of the Pocket Vault 102 and the website to determine what data should be transferred if synchronization is initiated. Software on the network server 114 may also or alternatively perform a similar comparison function automatically, if so desired.

Moreover, it should be understood that, in some embodiments, some of the above-noted functions may be performed without first requiring a Pocket Vault 102 to be authenticated. For example, some functions may involve the transfer of public or non-

sensitive data, and may not require protection via the authentication verification step 3302.

As shown in Fig. 33, when any of the above-listed seven functions is selected, either automatically or in response to user input, the selected function is performed. For each of functions 3314, 3316, 3318, 3320, 3322, and 3324, after performing the routine associated with the function, the routine 3024 proceeds to a step 3332, wherein it is determined whether the connection between the Pocket Vault 102 and the website on the network server 114 is still established.

When, at the step 3332, it is determined that the connection between the Pocket Vault 102 and the website on the network server 114 is still established, the routine 3024 returns to the step 3312 (discussed above).

When, at the step 3332, it is determined that the connection between the Pocket Vault 102 and the website on the network server 114 is no longer established, the routine 3024 proceeds to a step 3327, wherein some or all of the internet settings 2722 are ported from the interface station computer 304 to the Pocket Vault 102. The communication driver 3712 may cause the settings to be ported directly to the Pocket Vault 102 from the interface station computer 304 (via the interface unit 302), or the settings may be transferred first to the network server 114 and then to the Pocket Vault 102 (via the connection between the network server 114 and the Pocket Vault 102). In some embodiments, only certain types or classes of settings, e.g., certain type of cookies, PKI certificates, etc., are ported from the interface station computer 304 to the Pocket Vault 102 in this manner. The classes or types of settings that are ported during the step 3327 may, for example, be determined by the user in some embodiments. For example, the user may set certain preferences, e.g., during the SET PREFERENCES routine 3324 or by manipulating the Pocket Vault 102 directly, that control the nature and type of internet settings that are ported to the Pocket Vault 102 from the interface station computer 304 during the step 3327.

After the step 3327, the routine 3024 proceeds to a step 3328, wherein the communication driver 2712 causes the internet settings 2722 on the interface station computer 304 to return to their original state, i.e., the configuration the internet settings 2712 were in before they were altered in the step 3310.

After the step 3328, the routine 3024 proceeds to a step 3330, wherein any cached web pages or other information temporarily stored in the interface station computer 304

during the communication session between the Pocket Vault 102 and the website on the network server 114 are deleted from cache and other memory in the interface station computer 304. Thus, after completion of the step 3330, the interface station computer 304 is in essentially the same state it was in prior to the beginning of the routine 1422. The communication driver 2712 may remain on the interface station computer 304 or may be deleted in connection with the step 3330. If the communication driver 2712 is kept on the interface station computer 304, any cache or other memory associated with it that might store personal or sensitive information may also be erased. In some embodiments, the communication driver 2712 caches or stores very little, if any, information that is passed between the Pocket Vault 102 and the website on the network server 114. In any event, the communication driver 2712 may be constructed such that no useful data, i.e., data that reflects any personal or sensitive information, remains on it after completion of the step 3330.

When, at the step 3312, the holder chooses the TERMINATE SESSION function, the connection between the Pocket Vault 102 and the website on the network server 114 is de-established, and the routine 3024 proceeds immediately to the steps 3327, 3328 and 3330 (discussed above).

After the step 3330, the routine 3024 terminates.

Fig. 34 is a flow diagram illustrating an example implementation of the CARD LOADING routine 3314 shown in Fig. 33.

As shown, the routine 3314 begins at a step 3402, wherein a determination is made as to whether the card desired to be loaded is "swipeable." The user may, for example, be prompted to indicate whether the card has an operational magnetic stripe disposed thereon.

When, at the step 3402, the user indicates that the card does not have an operational magnetic stripe, the routine 3314 proceeds to a step 3406, wherein the user is prompted (e.g., via the browser on the interface station computer 304) to input information to be used in creating a card account.

When, at the step 3402, the user indicates that the card does have an operational magnetic stripe, the routine 3314 proceeds to the step 3410, wherein the user is prompted to swipe the card through the stripe reader 315 of the interface unit 302.

After the step 3406, the routine 3314 proceeds to steps 3408 and 3409, wherein it is determined whether the interface station computer 304 has received the information

from a card swiped through the stripe reader 315 of the interface unit 302 prior to the expiration of a timeout period.

When, at the step 3409, it is determined that the timeout period elapsed before information from a swiped card was received, the routine 3314 proceeds to a step 3411, wherein a message is displayed to the user concerning the failure to properly read the magnetic stripe.

After the step 3411, the routine 3314 returns to the step 3402 (discussed above). Thus, when a user is unsuccessful in swiping a card one or more times, the user may determine that the magnetic stripe is non-operational, and may indicate at the step 3402 that the card is not swipeable. The user may thereafter create an account for the card manually at the step 3410 (discussed above).

After the step 3410, the routine proceeds to a step 3412, wherein the website on the network server 114 determines whether the account for the card is valid. This determination may be made, for example, by confirming that the card is owned by the person attempting to add it to his or her Pocket Vault 102, that the card has not expired, etc.

When, at the step 3408, it is determined that information from the swiped card has been received prior to the expiration of the timeout period, the routine 3314 proceeds to the step 3412 (discussed above), wherein a determination is made as the validity of the account based upon the information read by the stripe reader 315.

When, at the step 3412, a determination is made that the account the user has requested to be added to the Pocket Vault 102 is not valid, the routine 3314 proceeds to a step 3414 wherein appropriate security precautions are taken.

After the step 3414, the routine 3314 terminates.

When, at the step 3412, a determination is made that the account the user has requested to be added to the Pocket Vault 102 is valid, the routine 3314 proceeds to a step 3416, wherein the information for the card is downloaded from the website on the network server 114 to the Pocket Vault 102 via the communication driver 2712.

After the step 3416, the routine 3314 proceeds to a step 3418, wherein a message is displayed that indicates the card has been successfully loaded onto the Pocket Vault 102 for use in future transactions.

After the step 3418, the routine 3314 terminates.

Fig. 35 is a flow diagram illustrating an example implementation of the SYNCHRONIZATION routine 3316 shown in Fig. 33.

As shown, the routine 3316 begins at a step 3502, wherein certain parameters required to synchronize the Pocket Vault 102 to the website on the network server 114 are determined based upon user preferences and the ID of the Pocket Vault 102. For example, if a holder has two or more Pocket Vaults 102, the holder may wish to elect one of them to be a master for synchronization purposes, or the holder may even elect to have the website act as the master. When a holder has more than one Pocket Vault 102, the holder also may desire to be prompted to select either the current date or the date of the last synchronization as the basis for the synchronization operation.

After the step 3502, the routine 3316 proceeds to a step 3504, wherein the website on the network server 114 generates sets of current data to transfer to the Pocket Vault 102. The website may, for example, compare its current data to the data stored on the Pocket Vault 102 so as to identify any data it needs to receive from the Pocket Vault 102 to properly synchronize therewith.

After the step 3504, the routine 3316 proceeds to steps 3506 and 3508, wherein it is determined whether the Pocket Vault 102 has indicated that it is ready to synchronize prior the expiration of a timeout period (measured by the step 3508). The Pocket Vault 102 may, for example, also be performing a similar comparison (e.g., using the synchronization module 2808) between its data and the data stored on the website of the network server to determine what data it needs to receive from the website to properly synchronize therewith.

When at the step 3508, it is determined that the timeout period has elapsed before the Pocket Vault 102 had indicated its readiness to synchronize, the routine 3316 proceeds to a step 3510, wherein a message is generated indicating the attempt to synchronize the Pocket Vault 102 with the website on the network server 114 has failed.

After the step 3510, the routine 3316 terminates.

When at the step 3506, it is determined that the Pocket Vault 102 has indicated its readiness to synchronize with the website prior to the expiration of the timeout period, the routine 3316 proceeds to a step 3512, wherein accumulated synchronization data is transferred from the website to the Pocket Vault 102, and vice versa, via the communication driver 2712.

After the step 3512, the routine 3316 proceeds to a step 3516, wherein the date of the successful synchronization is stored in both the Pocket Vault 102 and the network server 114.

After the step 3516, the routine 3316 proceeds to a step 3518, wherein a message is generated indicating that the Pocket Vault 102 has been successfully synchronized with the website on the network server 114.

After the step 3518, the routine 3316 terminates.

Figure 36 is a flow diagram illustrating an example implementation of the RECOVERY routine 3318 shown in Fig. 33.

As shown, the routine 3318 begins at a step 3602, wherein the website on the network server 114 compiles all data necessary to recover the Pocket Vault 102 to its state as of the last time its contents were synchronized with the website of the network server 114 (e.g., using the routine 3316 – described above) or backed up on the website of the network server 114 (e.g., using routine 3322 – described below).

After the step 3602, the routine 3318 proceeds to step 3604, wherein the data compile in the step 3602 is downloaded from the website on the network server 114 to the Pocket Vault 102 via the communication driver 2712, and a determination is made as to where that downloading has completed prior to the expiration of a timeout period measured at the step 3606.

When, at the step 3606, it is determined that the timeout period elapsed prior to the downloading being completed, the routine 3318 proceeds to a step 3608, wherein a message is generated indicating that the attempted recovery was unsuccessful.

After the step 3606, the routine 3318 terminates.

When, at the step 3606, it is determined that the downloading was completed in a timely manner, the routine 3318 proceeds to a step 3610, wherein a message is generated indicating that the attempted recovery of data to the Pocket Vault 102 was successful.

After the step 3610, the routine 3318 terminates.

Figure 37 is a flow diagram illustrating an example implementation of the IDENTITY PORTING SELECTION routine 3320 shown in Fig. 33.

As shown, the routine 3320 begins at a step 3702, wherein the internet settings 2722 from the interface station computer 304 are downloaded from the interface station computer 304 to the website on the network server 114.

After the step 3702, the routine 3320 proceeds to a step 3704, wherein the website on the network server 114 compiles and displays the downloaded internet settings to the user via the browser on the interface station computer 304. The settings may be displayed to the user in any of a number of ways. Preferably, the settings are displayed in a manner that enables the user to readily distinguish between various classes of settings, and that permits the user to readily identify the purpose of each type of setting. In some embodiments, only a subset of the all of the internet settings 2722 (e.g., only settings such as cookies and PKI certificates) are transferred to the website for possible modification by the user.

After the step 3704, the routine 3320 proceeds to steps 3706 and 3708, wherein the user is given an opportunity to modify the displayed internet settings. The user may, for example, elect to keep certain cookies that were retained among the internet settings 2722, while choosing to discard others.

When at the step 3708, the user has indicated that he or she has completed any modifications of the retrieved internet settings 2722, the routine 3320 proceeds to a step 3710, wherein the modified internet settings are downloaded from the website on the network server 114 to the Pocket Vault 102 via the communication driver 2712.

After the step 3710, the routine 3320 terminates.

When at the step 3706, it is determined that the user did not elect to modify any settings, the routine 3320 terminates.

Figure 38 is a flow diagram illustrating an example implementation of the BACKUP routine 3322 shown in Fig. 33.

As shown, the routine 3322 begins at a step 3802, wherein the website on the network server 114 transmits a request to the Pocket Vault 102 via the communication driver 2712, asking the Pocket Vault 102 to send the website backup data. This backup data may, for example, constitute all data necessary to place the Pocket Vault 102 back into its present state if any portion of data on the Pocket Vault 102 was lost, or to place a new Pocket Vault 102 into the same state as the backed up Pocket Vault 102 (e.g., using the RECOVERY routine 3318 – discussed above).

After the step 3802, the routine 3322 proceeds to steps 3804 -3806, wherein it is determined whether the requested backup data has been successfully transferred from the Pocket Vault 102 to the website on the network server 114 before the expiration of a timeout period (measured by the step 3806).

When, at the step 3806, it is determined that the timeout period elapsed prior to the backup data being successfully transferred, the routine 3322 proceeds to a step 3808, wherein a message is displayed (e.g., via the browser on the interface station computer 304) informing the user that a communication error has occurred and that the backup operation was unsuccessful.

After the step 3808, the routine 3322 terminates.

When, at the step 3804, the routine 3322 determined that, before the timeout period, the backup data has been successfully transferred from the Pocket Vault 102 to the website on the network server 114 via the communication driver 2712, the routine 3322 proceeds to a step 3810, wherein the received backup data is stored by the network server 114, e.g., for use in connection with the RECOVERY routine 3318.

After the step 3310, the routine 3322 proceeds to a step 3812, wherein a message is displayed (e.g., via the browser on the interface station computer 304) informing the user that the backup operation was successfully completed.

After the step 3312, the routine 3322 terminates.

Figure 39 is a flow diagram illustrating an example implementation of the SET PREFERENCES routine 3324 shown in Fig. 33. The SET PREFERENCES routine 3324 permits the holder to set or alter preferences on his or her Pocket Vault 102 using a browser on the interface station computer 104.

As shown, the routine 3324 begins at a step 3902, wherein the website on the network server 114 transmits a request to the Pocket Vault 102 via the communication driver 2712, requesting the Pocket Vault 102 to transmit all "preferences" information stored on the Pocket Vault 102 to the website on the network server 114 via the communication driver 2712. This information may, for example, comprise definitions of home pages, connection of secure and non-secure media, order of media presentment, sort orders, user interface options, synchronization defaults, etc.

After the step 3902, the routine 3324 proceeds to steps 3904 and 3906, wherein it is determined whether the preferences information has been received from the Pocket Vault 102 prior to the expiration of a timeout period (measured by the step 3906).

When, at the step 3906, it is determined that the timeout period elapsed before the preferences information was transferred from the Pocket Vault 102 to the website, the routine 3324 proceeds to a step 3908, wherein a message is displayed (e.g., on the browser) indicating that a communication error has occurred.

After the step 3908, the routine 3324 terminates.

When, at the step 3904, it is determined that the preferences information has been successfully transferred from the Pocket Vault 102 to the website on the network server 114, the routine 3324 proceeds to a step 3910, wherein the website compiles and displays the current preference settings for the Pocket Vault 102 (e.g., on the browser) in a user friendly manner.

After the step 3910, the routine 3324 proceeds to steps 3912 and 3914, wherein the user is given an opportunity to modify the displayed preference settings.

When, at the step 3912, the user opts not to modify any of the displayed settings, the routine 3324 terminates.

When, at the steps 3912 and 3914, the user opts to modify the displayed settings and indicates that he or she has completed modification thereof, the routine 3324 proceeds to a step 3916, wherein the modified preference settings are downloaded from the website on the network server 114 to the Pocket Vault 102 via the communication driver 2712.

After the step 3918, a message is displayed (e.g., via the browser on the interface station computer 304) informing the user that the preference settings for the Pocket Vault 102 were successfully modified.

After the step 3918, the routine 3324 terminates.

Fig. 40 is a flow diagram illustrating an example implementation of the RFID TAG LOADING routine 3315 shown in Fig. 33.

As shown, the routine 3315 begins at a step 4002, wherein the user may use the website on the network server 114 to create an account for the RFID tag to be loaded onto the Pocket Vault 102.

After the step 4002, the routine proceeds to a step 4004, wherein the website on the network server 114 determines whether the account for the RFID tag is valid, for example, by checking with the media that issued the RFID tag account.

When, at the step 4004, it is determined that the account for the RFID tag is not valid, the routine 3315 proceeds to a step 4010, wherein appropriate security precautions are taken.

After the step 4010, the routine 3315 terminates.

When, at the step 4004, a determination is made that the account for the RFID tag is valid, the routine 3315 proceeds to a step 4006, wherein the information for the RFID

tag is downloaded from the website on the network server 114 to the Pocket Vault 102 via the communication driver 2712.

After the step 4006, the routine 3315 proceeds to a step 4008, wherein a message is displayed that indicates the RFID tag information has been successfully loaded onto the Pocket Vault 102 for use in future transactions.

After the step 4008, the routine 3315 terminates.

One illustrative example of an application of the network system described herein is in the distribution of building access key cards and similar limited-use, time-sensitive media to individual operators. The following typical scenario involves distribution of hotel room key cards to hotel guests who make room reservations over the Internet. Using a hotel's secure web site, the prospective guest, who is also a Pocket Vault holder, may secure a room for a specific time period by providing a credit card number. This step may or may not involve use of a credit card stored on the Pocket Vault 102. If it does involve use of a Pocket Vault credit card, this card may, for example, be accessed while the Pocket Vault 102 is interfaced with the holder's personal interface station 104b. Next, the prospective hotel guest may link to the network server 114 (while staying within the hotel's website), and follow on-screen instructions for downloading the key card for his/her room onto the Pocket Vault 102 (e.g., to ensure that the Pocket Vault 102 is interfaced with the pocket vault interface unit 302, and to ensure that the Pocket Vault holder has activated the Pocket Vault 102 by the appropriate security mechanism such as a thumbprint for bio-metric ID verification). After downloading is complete, the display 216 of the Pocket Vault 102 may include an icon for the hotel room key (e.g., the hotel's logo), along with the icons for media previously loaded. When the room key card icon is selected, the Pocket Vault 102 may encode the Chameleon Card with the magnetic stripe coding to unlock the guest's hotel room.

After the time period of the guest's room reservation has expired, the Pocket Vault 102 may automatically delete the room key icon. This deletion may occur for the convenience of the Pocket Vault holder, not necessarily for hotel security reasons, since the room's lock will reject any previously-used key card (Chameleon or traditional key card) after the key card's specified time period has expired.

Having thus described at least one illustrative embodiment of the invention, various alterations, modifications and improvements will readily occur to those skilled in the art. Such alterations, modifications and improvements are intended to be within the

spirit and scope of the invention. Accordingly, the foregoing description is by way of example only and is not intended as limiting. The invention is limited only as defined in the following claims and the equivalents thereto.

What is claimed is:

CLAIMS

1. An apparatus, comprising:

a user authenticator that authenticates an identity of a user; and

a transponder that is permitted to emit a wireless signal representing information stored in the apparatus in response to a wireless interrogation signal after the user authenticator has authenticated the identity of the user.

2. The apparatus of claim 1, wherein the wireless signal representing the information and the wireless interrogation signal are radio frequency signals.

3. The apparatus of claim 1 or 2, wherein the apparatus further comprises a memory that stores at least first and second distinct codes, and a user input that permits the user to select any one of the at least first and second codes for transmission in response to an interrogation signal; and wherein the transponder is permitted to emit a wireless signal representing the selected one of the at least first and second codes in response to an interrogation signal.

4. The apparatus of claim 3, further comprising a display that identifies the one of the at least first and second codes the user has selected.

5. The apparatus of claim 3 or 4, wherein the first and second codes correspond to accounts the user holds with respective first and second unrelated media issuers.

6. The apparatus of any one of claims 1-5, in combination with an interrogator that wirelessly emits the interrogation signal, and receives from the apparatus the wireless signal representing the information.

7. An apparatus, comprising:

a memory that stores at least first and second distinct codes;

a user input that permits a user to select any one of the at least first and second codes for transmission in response to a wireless interrogation signal; and

a transponder that emits a wireless signal representing the selected one of the at least first and second codes in response to an interrogation signal.

8. The apparatus of claim 7, wherein the wireless signal representing the identification information and the wireless interrogation signal are radio frequency signals.

9. The apparatus of claim 7 or 8, further comprising a display that identifies the one of the at least first and second codes the user has selected.

10. The apparatus of any one of claims 7-9, wherein the first and second codes correspond to accounts the user holds with respective first and second unrelated media issuers.

11. The apparatus of any one of claims 7-10, in combination with an interrogator that wirelessly emits the interrogation signal, and receives from the apparatus the wireless signal representing the selected one of the at least first and second codes.

12. A token that may be used to engage in a transaction at a point of sale, comprising:

a substrate;

a rewriteable memory, supported by the substrate, that can be selectively configured to store information on the token that identifies an account that is to be used to engage in the transaction at the point of sale, the substrate and memory being configured and arranged such that the substrate can be selectively interfaced with an apparatus at the point of sale to permit the apparatus to read the contents of the memory; and

a reconfigurable display, supported by the substrate, that displays at least some of the information that is stored in the rewritable memory.

13. The token of claim 12, wherein rewritable memory stores both an account identifier and a security code separate from the account identifier, and the reconfigurable display displays both the account identifier and the security code.

14. The token of claim 12 or 13, wherein the substrate is substantially the size of a credit card.

15. The token of any one of claims 12-14, wherein the rewritable memory comprises means for selectively storing information on the token that identifies an account that is to be used to engage in the transaction at the point of sale.

16. The token of any one of claims 12-15, wherein the rewritable memory comprises a rewriteable magnetic stripe.

17. The token of any one of claims 12-15, wherein the rewritable memory comprises a circuit that simulates a magnetic stripe.

18. The token of any one of claims 12-15, wherein the rewritable memory comprises a circuit that simulates an account number storage mechanism of a Smartcard.

19. The token of any one of claims 12-18, wherein the reconfigurable display comprises a liquid crystal display (LCD).

20. The token of claim 19, wherein the LCD is flexible.

21. The token of any one of claims 12-29, in combination with an apparatus to which the token is releasably attached, the apparatus being configured to cause the rewritable memory of the token to store the information and to cause the display of the token to display at least some of the information after the token is detached from the apparatus.

22. The combination of claim 21, wherein the rewritable memory comprises means for selectively storing information on the token that identifies an account that is to be used to engage in the transaction at the point of sale.

23. The combination of claim 21 or 22, wherein the apparatus to which the token is releasably attached comprises a memory that stores at least first information identifying a first account and second information identifying a second account, and a user input that permits the user to select one of the first information and second information for use in the transaction, and wherein the apparatus is further configured to cause the rewritable memory of the token to store the selected one of the first information and second information and to cause the display of the token to display at least some of the selected one of the first information and second information.

24. The combination of claim 23, further comprising a display that identifies the one of the first information and second information the user has selected.

25. The combination of claim 23 or 24, wherein the first information and second information correspond to accounts the user holds with respective first and second unrelated media issuers.

26. A method for using an apparatus, comprising steps of:

using the apparatus to authenticate an identity of a user of the apparatus; and

after the apparatus has authenticated the identity of the user, enabling a transponder of the apparatus to emit a wireless signal representing information stored in the apparatus in response to a wireless interrogation signal.

27. The method of claim 26, wherein the wireless signal representing the information and the wireless interrogation signal are radio frequency signals.

28. The method of claim 26 or 27, wherein the method further comprises steps of:

manipulating a user input on the apparatus to select one of at least first and second codes stored in memory; and

permitting the transponder to emit a wireless signal representing the selected one of the first and second codes in response to the interrogation signal.

29. The method of claim 28, wherein the method further comprises steps of:

manipulating the user input on the apparatus to select the other of the first and second codes stored in memory; and

permitting the transponder to emit a wireless signal representing the other of the first and second codes in response to the interrogation signal.

30. The method of claim 28 or 29, further comprising a step of:

in response to the user manipulating the user input, displaying to the user an identification of the one of the first and second codes the user has selected.

31. The method of any one of claims 28-30, wherein the first and second codes correspond to accounts the user holds with respective first and second unrelated media issuers.

32. The method of any one of claims 26-31, further comprising steps of:

wirelessly emitting an interrogation signal from an interrogator;

receiving the interrogation signal at the transponder;

in response to receiving the interrogation signal, emitting from the transponder a wireless signal representing the information; and

receiving at the interrogator the wireless signal representing the information.

33. The method of claim 32, further comprising a step of authorizing a transaction based upon the information received at the interrogator.

34. A method for using an apparatus, comprising steps of:

manipulating a user input on the apparatus to select one of at least first and second codes stored in memory; and

permitting a transponder of the apparatus to emit a wireless signal representing the selected one of the at least first and second codes in response to a wireless interrogation signal.

35. The method of claim 34, wherein the wireless signal representing the selected one of the at least first and second codes and the wireless interrogation signal are radio frequency signals.

36. The method of claim 34 or 35, wherein the method further comprises steps of:

manipulating the user input on the apparatus to select another of the at least first and second codes stored in memory; and

permitting the transponder to emit a wireless signal representing the other of the at least first and second codes in response to the wireless interrogation signal.

37. The method of any one of claims 34-36, further comprising a step of:

in response to the user manipulating the user input, displaying to the user an identification of the one of the at least first and second codes the user has selected.

38. The method of any one of claims 34-37, wherein the first and second codes correspond to accounts the user holds with respective first and second unrelated media issuers.

39. The method of any one of claims 34-38, further comprising steps of:

wirelessly emitting an interrogation signal from an interrogator;

receiving the interrogation signal at the transponder;

in response to receiving the interrogation signal, emitting from the transponder a wireless signal representing the selected one of the at least first and second codes; and

receiving at the interrogator the wireless signal representing the selected one of the at least first and second codes.

40. The method of claim 39, further comprising a step of authorizing a transaction based upon the selected one of the at least first and second codes received at the interrogator.

41. A method for configuring a token to be used to engage in a transaction at a point of sale, comprising steps of:

configuring a rewritable memory of the token to store information that identifies an account that may be used to engage in the transaction at the point of sale, the memory being configured and arranged on the token such that the token can be selectively interfaced with an apparatus at the point of sale to permit the apparatus to read the contents of the memory; and

configuring a display on the token to display at least some of the information that is stored in the rewritable memory.

42. The method of claim 41, wherein the step of configuring the rewritable memory includes a step of configuring the rewritable memory to store both an account identifier and a security code separate from the account identifier, and the step of configuring the display includes configuring the display to display both the account identifier and the security code.

43. The method of claim 41 or 42, wherein the token is substantially the size of a credit card.

44. The method of any one of claims 41-43, wherein the step of configuring the rewritable memory includes using a magnetic head to configure a rewriteable magnetic stripe on the token.

45. The method of any one of claims 41-43, wherein the step of configuring the rewritable memory includes configuring the rewritable memory to cause a simulated magnetic stripe to be generated on the token.

46. The method of any one of claims 41-43, wherein the step of configuring the rewritable memory includes configuring the rewritable memory to simulate an account number storage mechanism of a Smartcard.

47. The method of any one of claims 41-46, wherein:

the method further comprises a step of manipulating a user input to select one of at least first information identifying a first account and second information identifying a second account;

the step of configuring the rewritable memory includes configuring the rewritable memory to store the selected one of the at least first information and second information; and

the step of configuring the display includes configuring the display to display at least some of the selected one of the at least first information and second information.

48. The method of claim 47, further comprising a step of displaying to the user an identification of the one of the at least first information and second information the user has selected.

49. The method of claim 47 or 48, wherein the first information and second information correspond to accounts the user holds with respective first and second unrelated media issuers.

50. The method of any one of claims 41-49, further comprising steps of:

interfacing the token with an apparatus at the point of sale to permit the apparatus to read the contents of the memory;

displaying the information read from the memory on a display of the apparatus; and

comparing the information displayed on the display of the token with the information displayed on the display of the apparatus to verify the authenticity of the token.

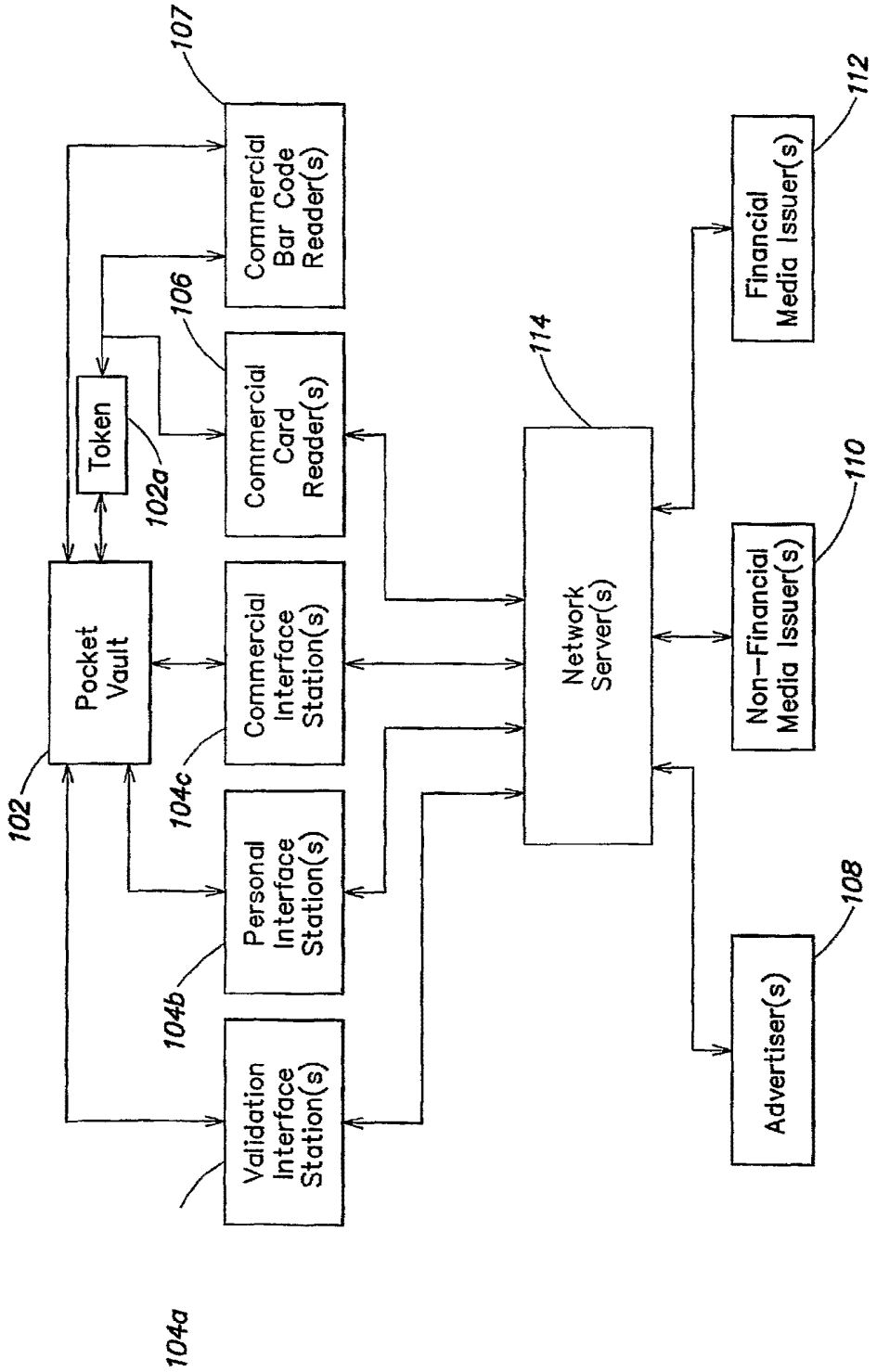

Pocket Vault
102
Token
102a
Commercial Bar Code Reader(s)
107
Commercial Card Reader(s)
106
Commercial Interface Station(s)
104c
Personal Interface Station(s)
104b
Validation Interface Station(s)
104a
Network Server(s)
114
Financial Media Issuer(s)
112
Non-Financial Media Issuer(s)
110
Advertiser(s)
108

FIG. 1

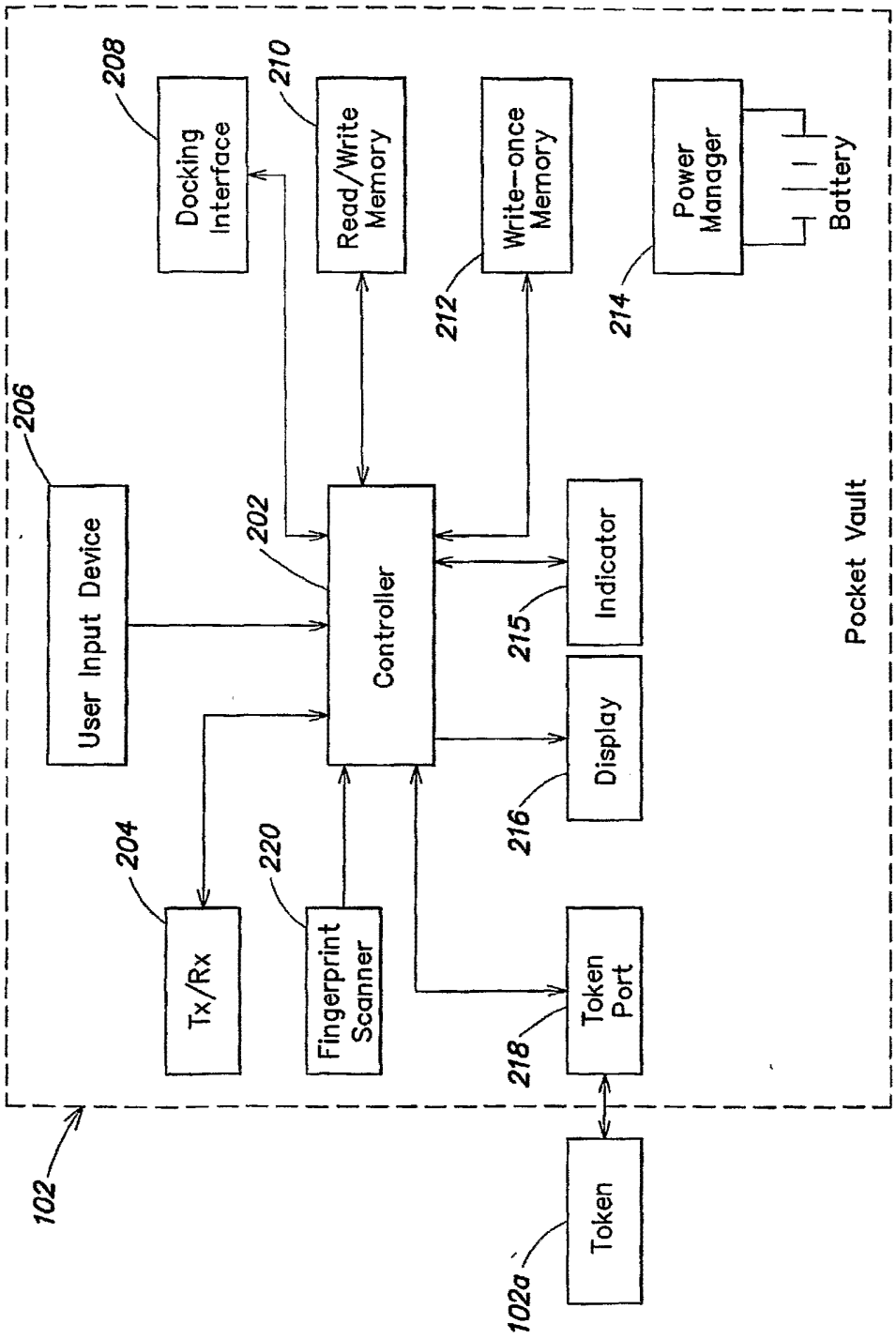

208
Docking Interface
210
Read/Write Memory
Write-once Memory
212
Power Manager
214
Battery
206
User Input Device
202
Controller
Indicator
215
Display
216
Pocket Vault
204
Tx/Rx
220
Fingerprint Scanner
218
Token Port
102
Token
102a

FIG. 2

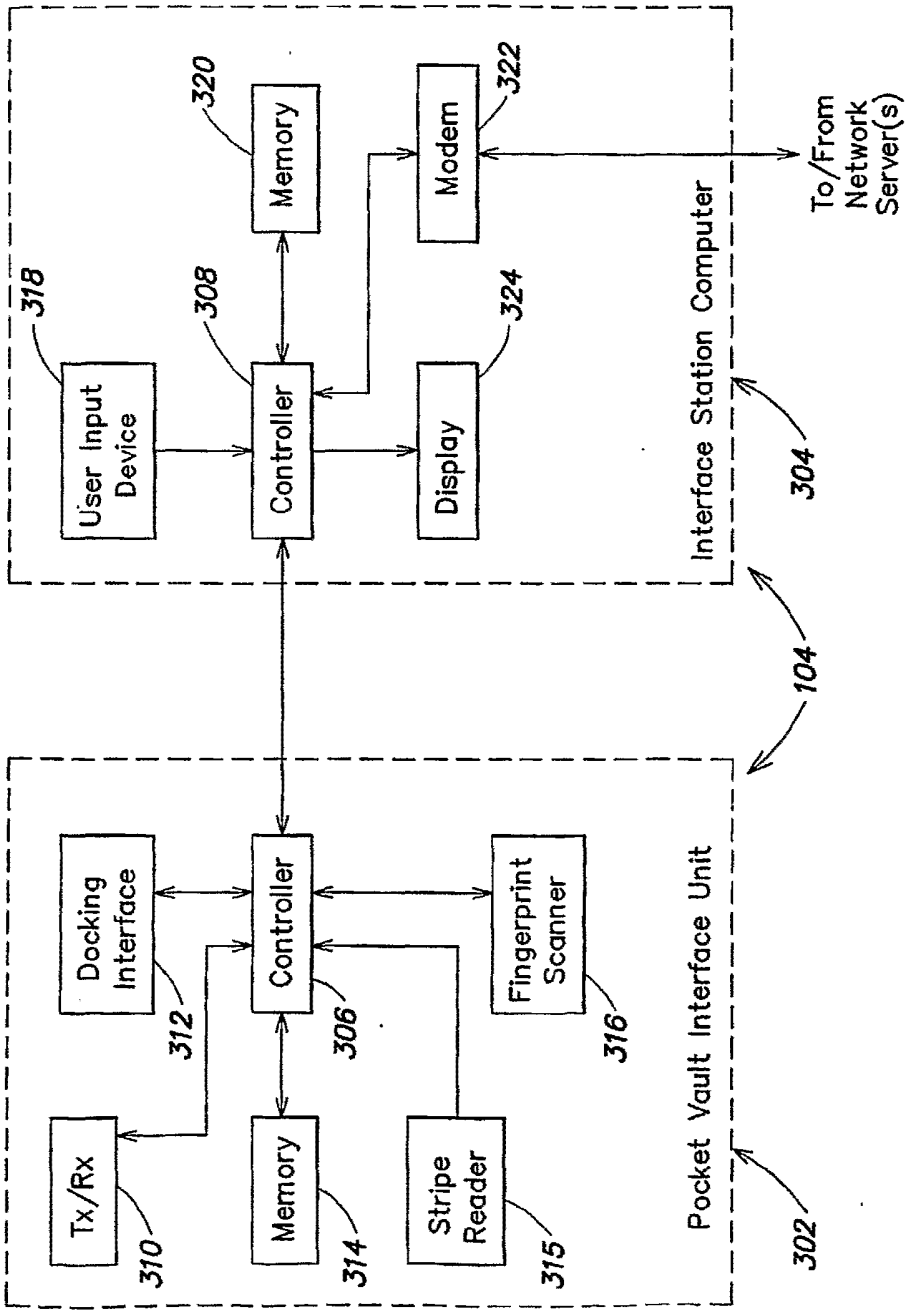

Interface Station Computer
304
User Input Device
318
Controller
308
Memory
320
Display
324
Modem
322
To/From Network Server(s)
104
Pocket Vault Interface Unit
302
Docking Interface
312
Controller
306
Fingerprint Scanner
316
Tx/Rx
310
Memory
314
Stripe Reader
315

FIG. 3

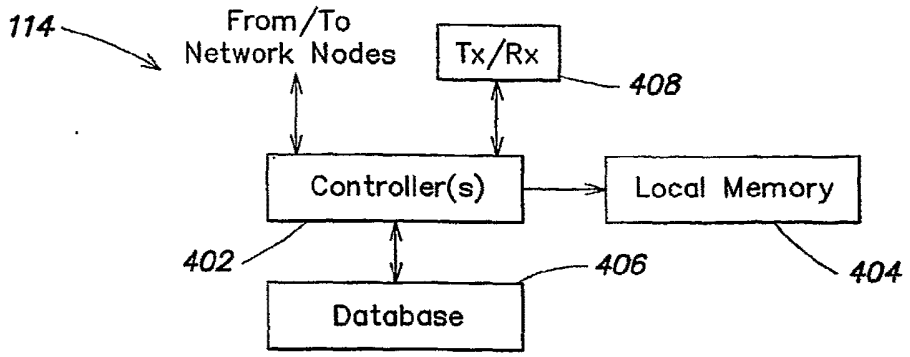


FIG. 4

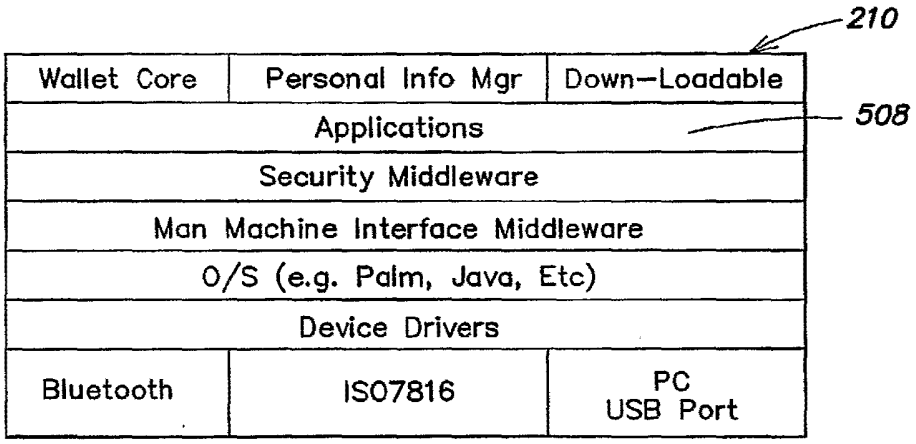


FIG. 5

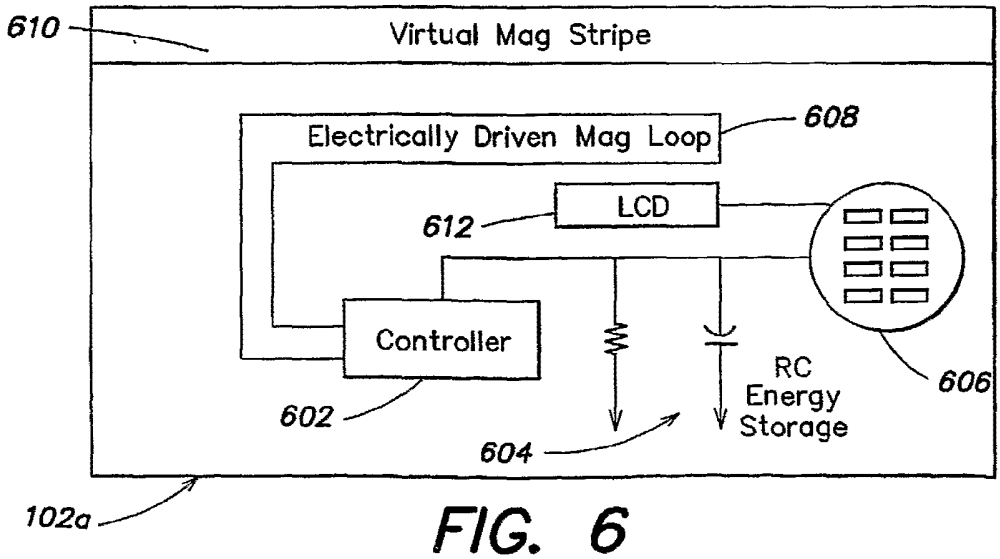


FIG. 6

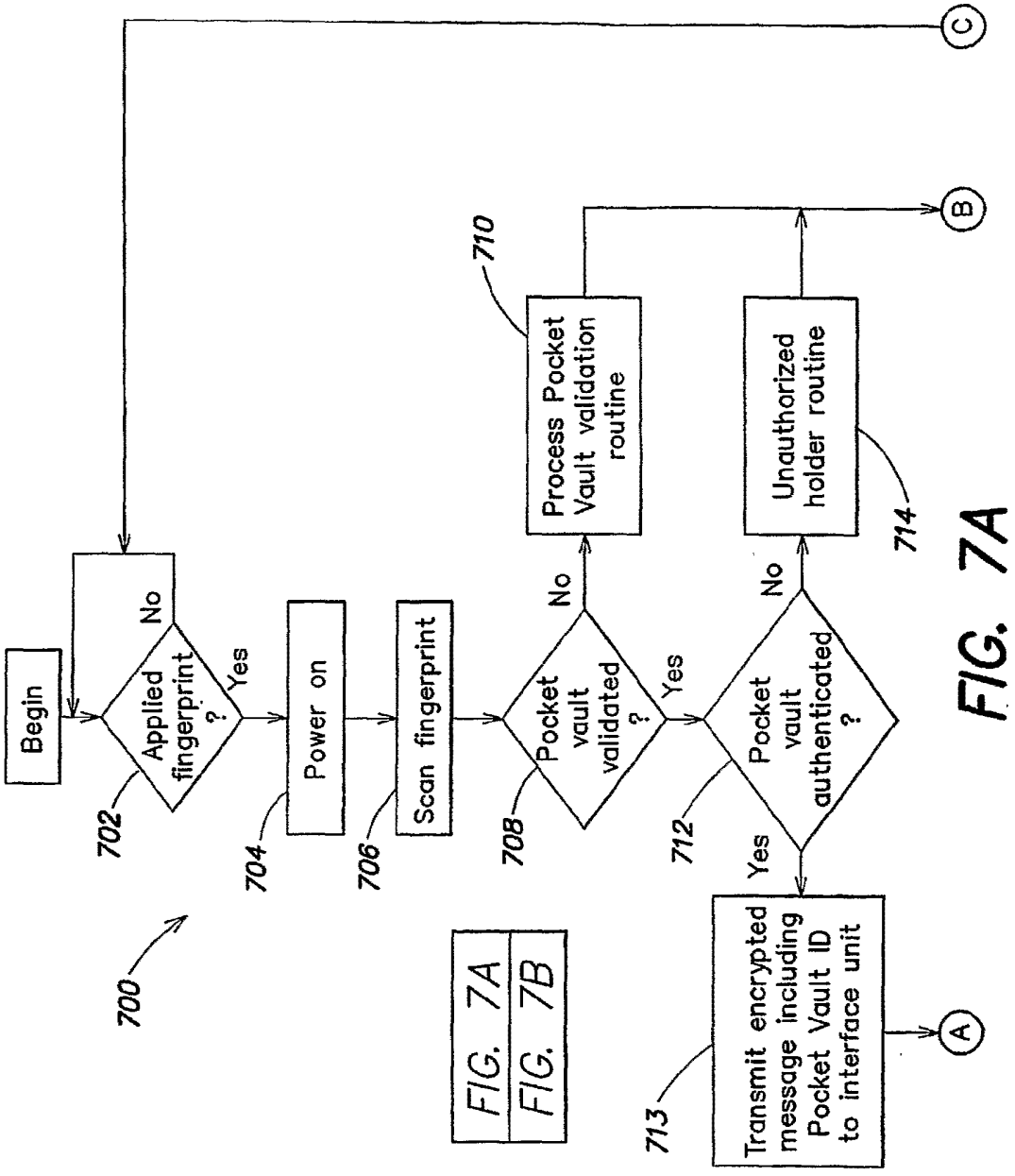


FIG. 7A

FIG. 7A
FIG. 7B

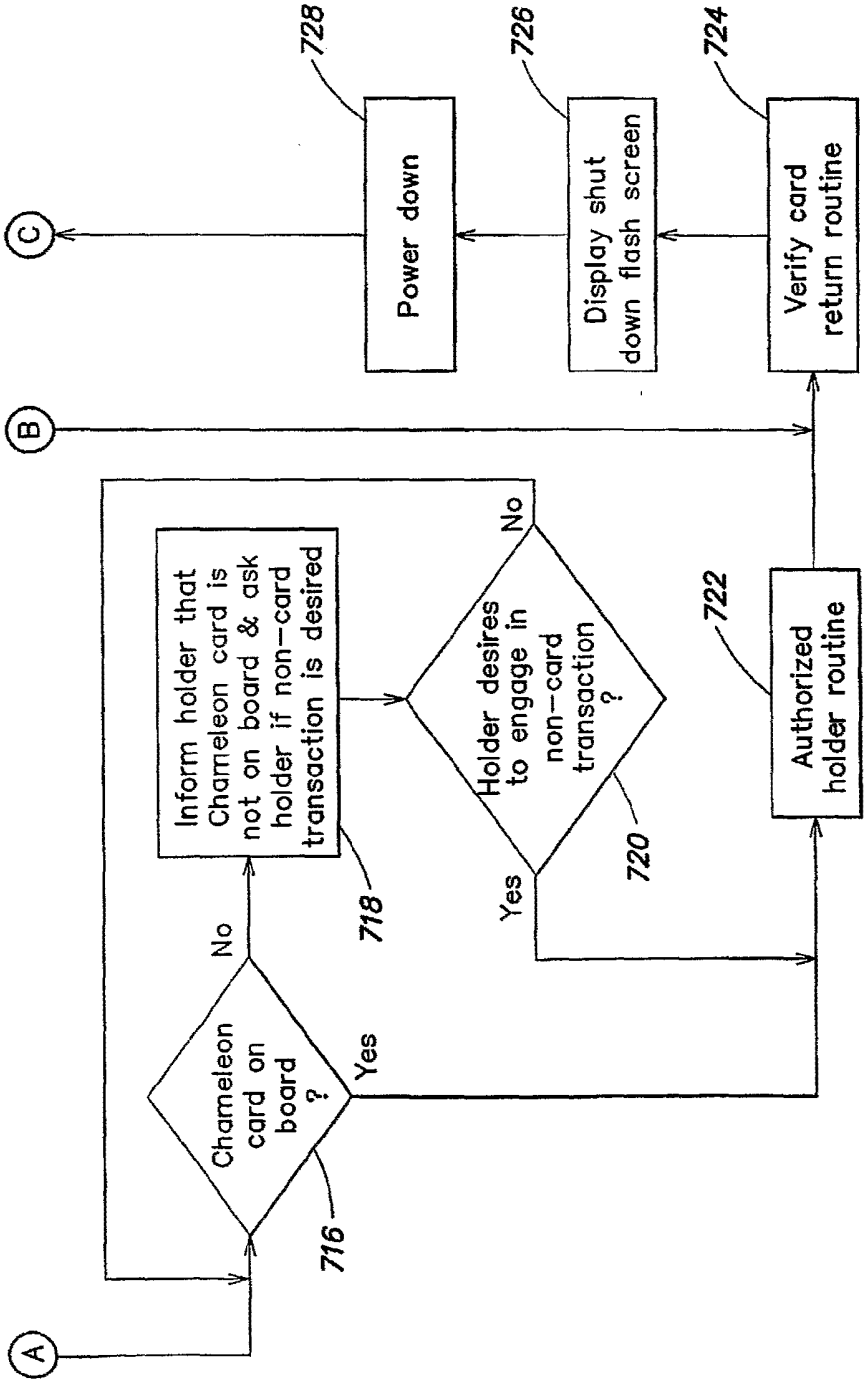

A
B
C
Chameleon card on board ?
716
No
Yes
Inform holder that Chameleon card is not on board & ask holder if non-card transaction is desired
718
Holder desires to engage in non-card transaction ?
720
No
Yes
Authorized holder routine
722
Verify card return routine
724
Display shut down flash screen
726
Power down
728

FIG. 7B

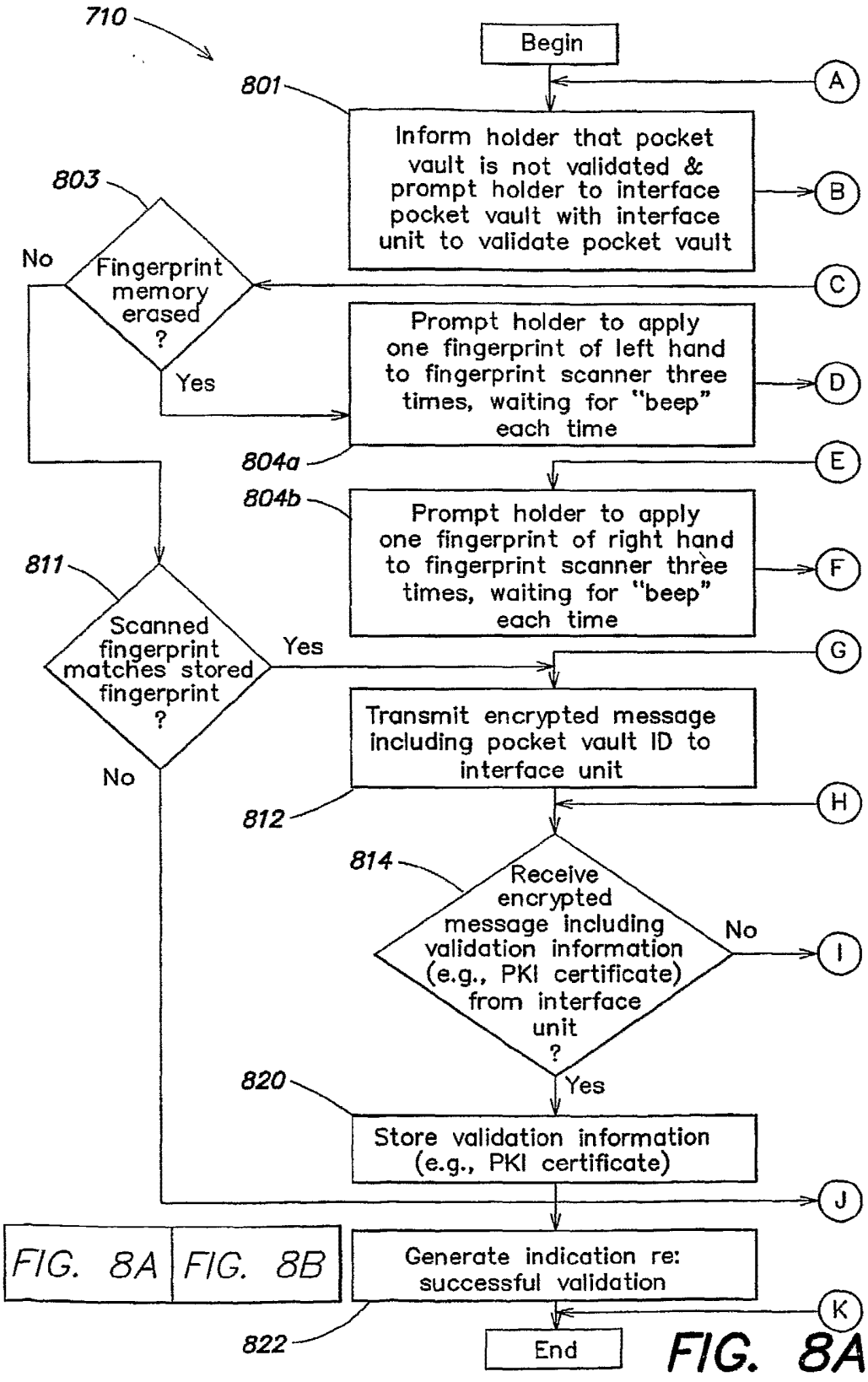


FIG. 8A | FIG. 8B

FIG. 8A

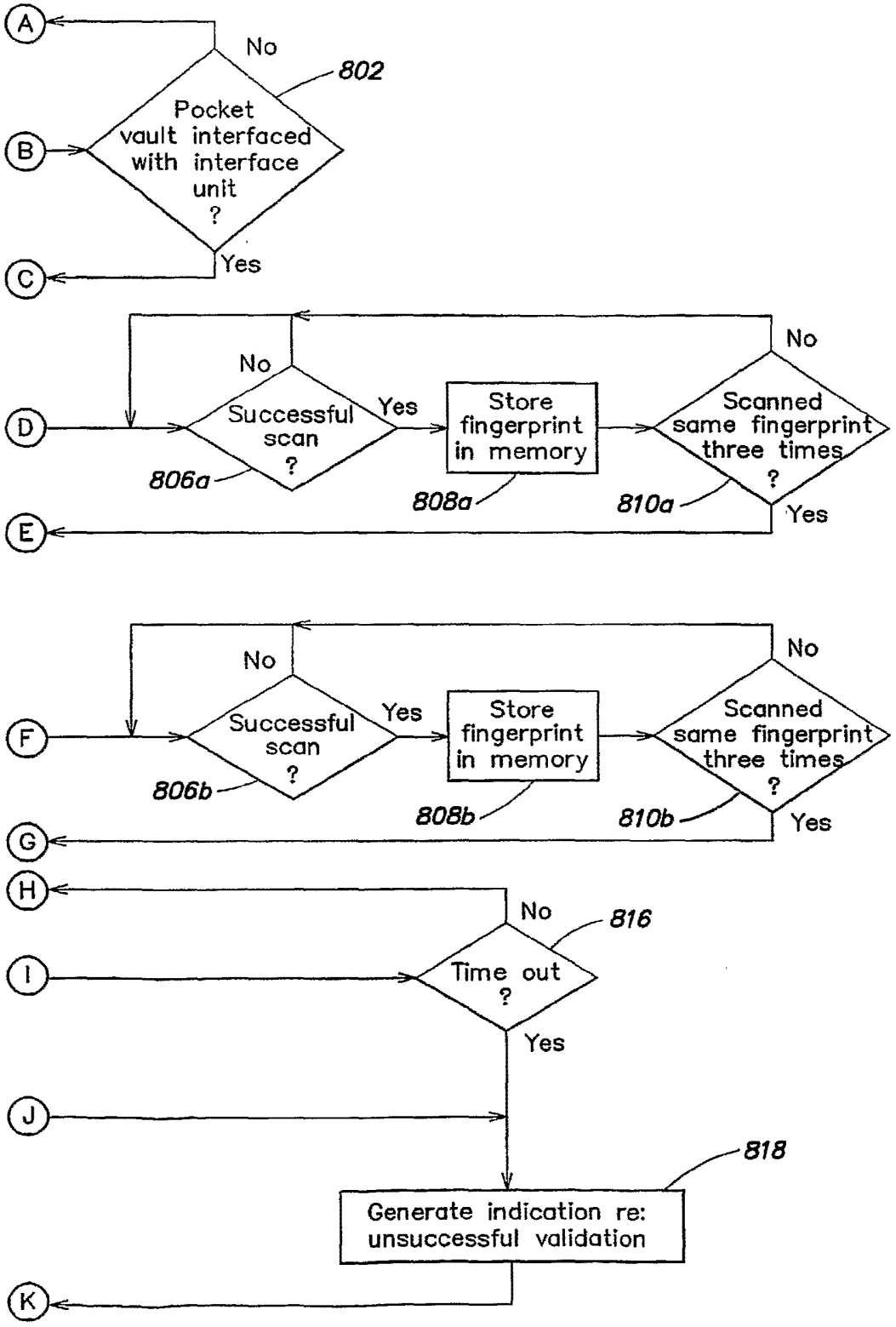

A
No
802
Pocket vault interfaced with interface unit ?
B
Yes
C
No
No
D
Successful scan ?
Yes
Store fingerprint in memory
Scanned same fingerprint three times ?
806a
808a
810a
Yes
E
No
No
F
Successful scan ?
Yes
Store fingerprint in memory
Scanned same fingerprint three times ?
806b
808b
810b
Yes
G
H
No
816
I
Time out ?
Yes
J
818
Generate indication re: unsuccessful validation
K

FIG. 8B

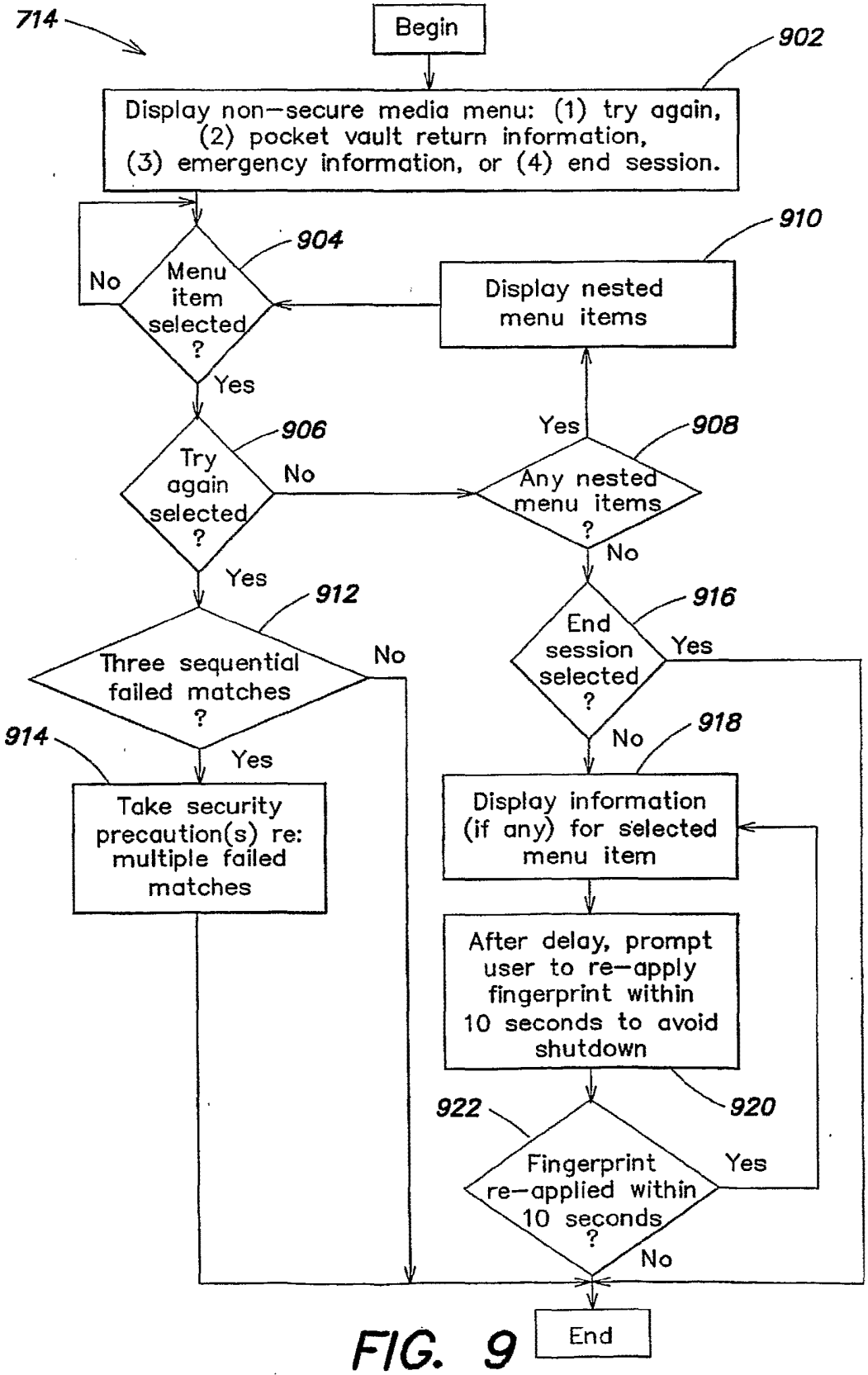

714
Begin
902
Display non-secure media menu: (1) try again, (2) pocket vault return information, (3) emergency information, or (4) end session.
904
Menu item selected ?
No
Yes
910
Display nested menu items
906
Try again selected ?
No
Yes
908
Any nested menu items ?
Yes
No
912
Three sequential failed matches ?
No
Yes
914
Take security precaution(s) re: multiple failed matches
916
End session selected ?
Yes
No
918
Display information (if any) for selected menu item
After delay, prompt user to re-apply fingerprint within 10 seconds to avoid shutdown
920
922
Fingerprint re-applied within 10 seconds ?
Yes
No
End

FIG. 9

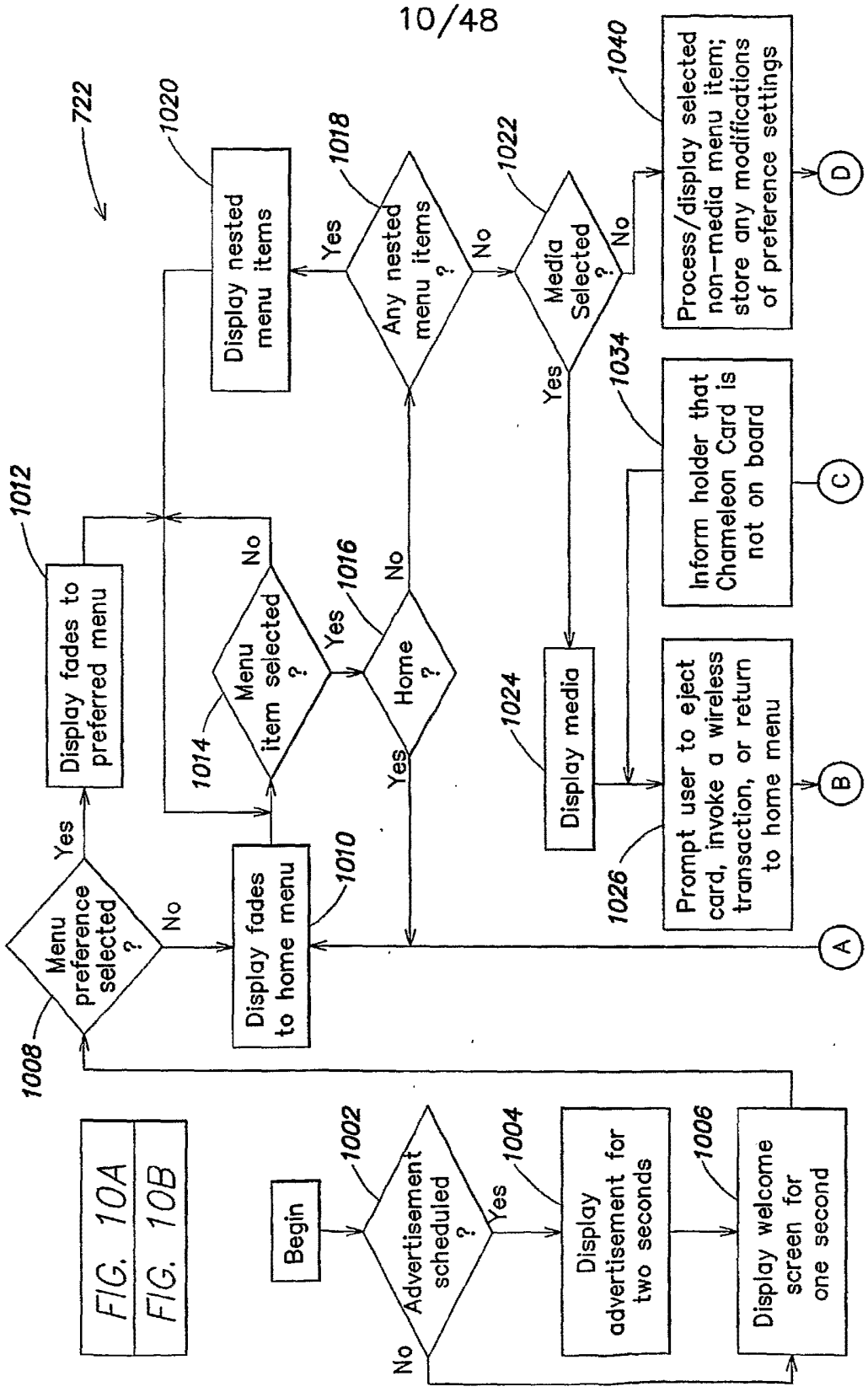


FIG. 10A

FIG. 10A
FIG. 10B

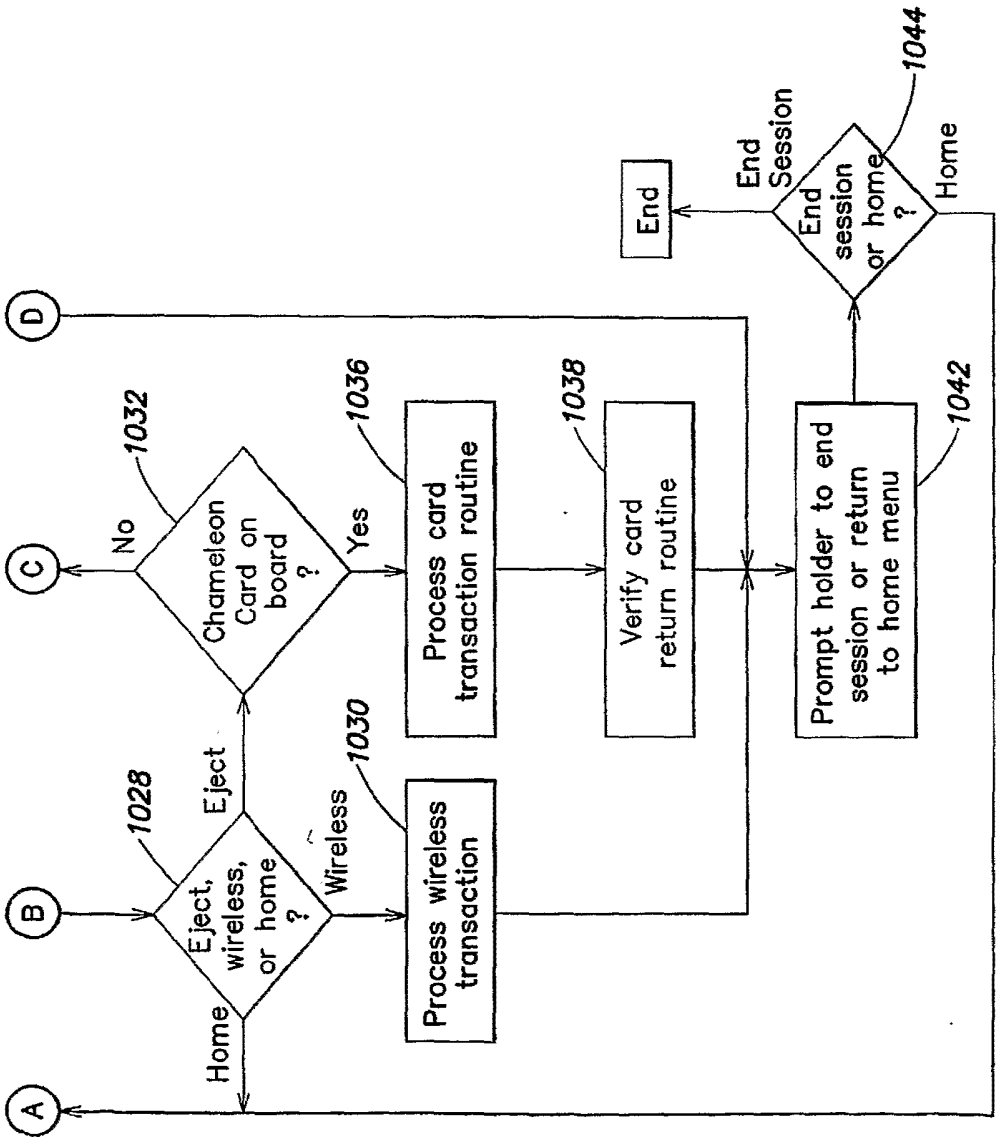

A
B
C
D
Home
Eject, wireless, or home ?
1028
Eject
Wireless
Process wireless transaction
1030
Chameleon Card on board ?
1032
No
Yes
Process card transaction routine
1036
Verify card return routine
1038
Prompt holder to end session or return to home menu
1042
End session or home ?
1044
End Session
Home
End

FIG. 10B

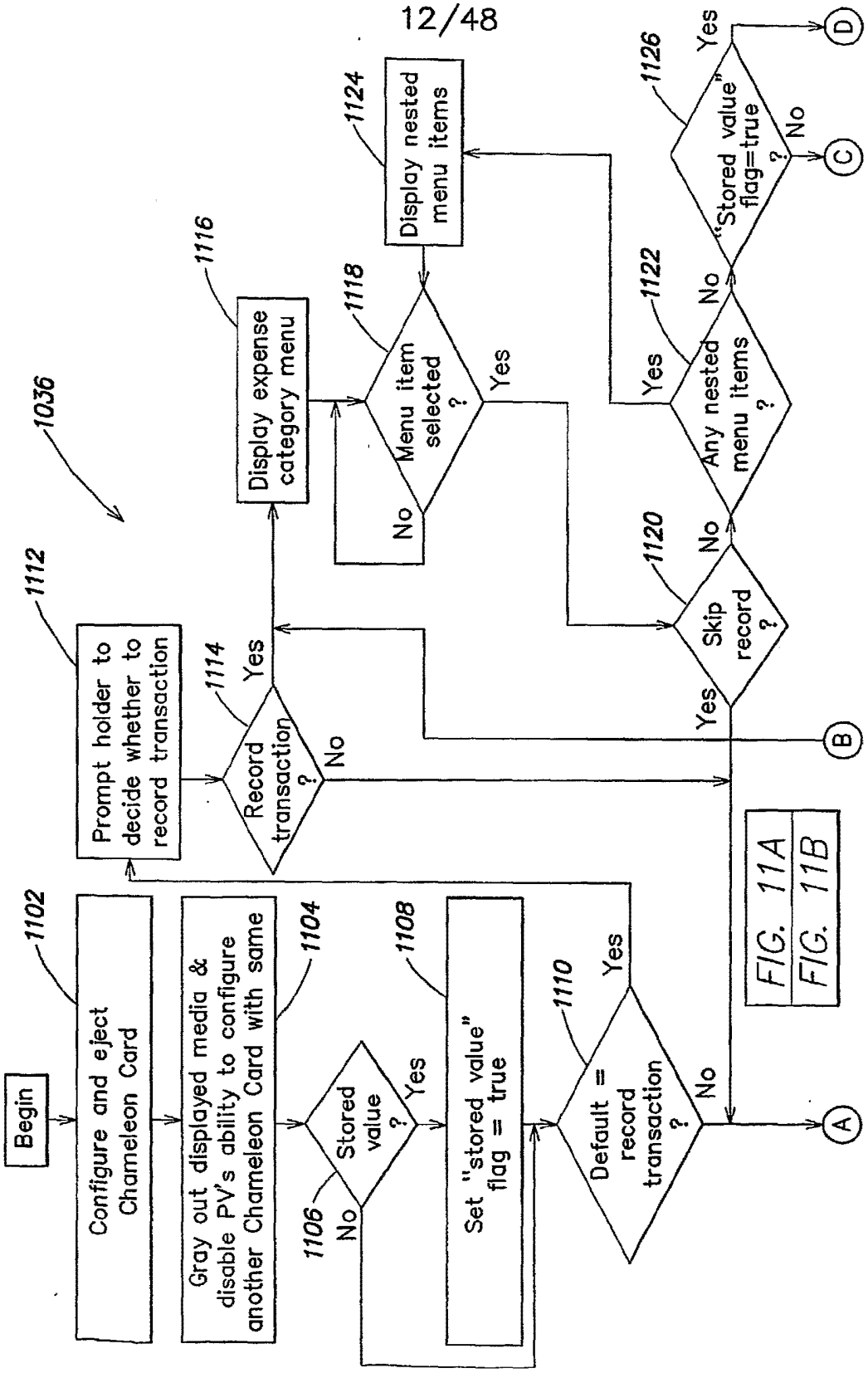


FIG. 11A

FIG. 11A
FIG. 11B

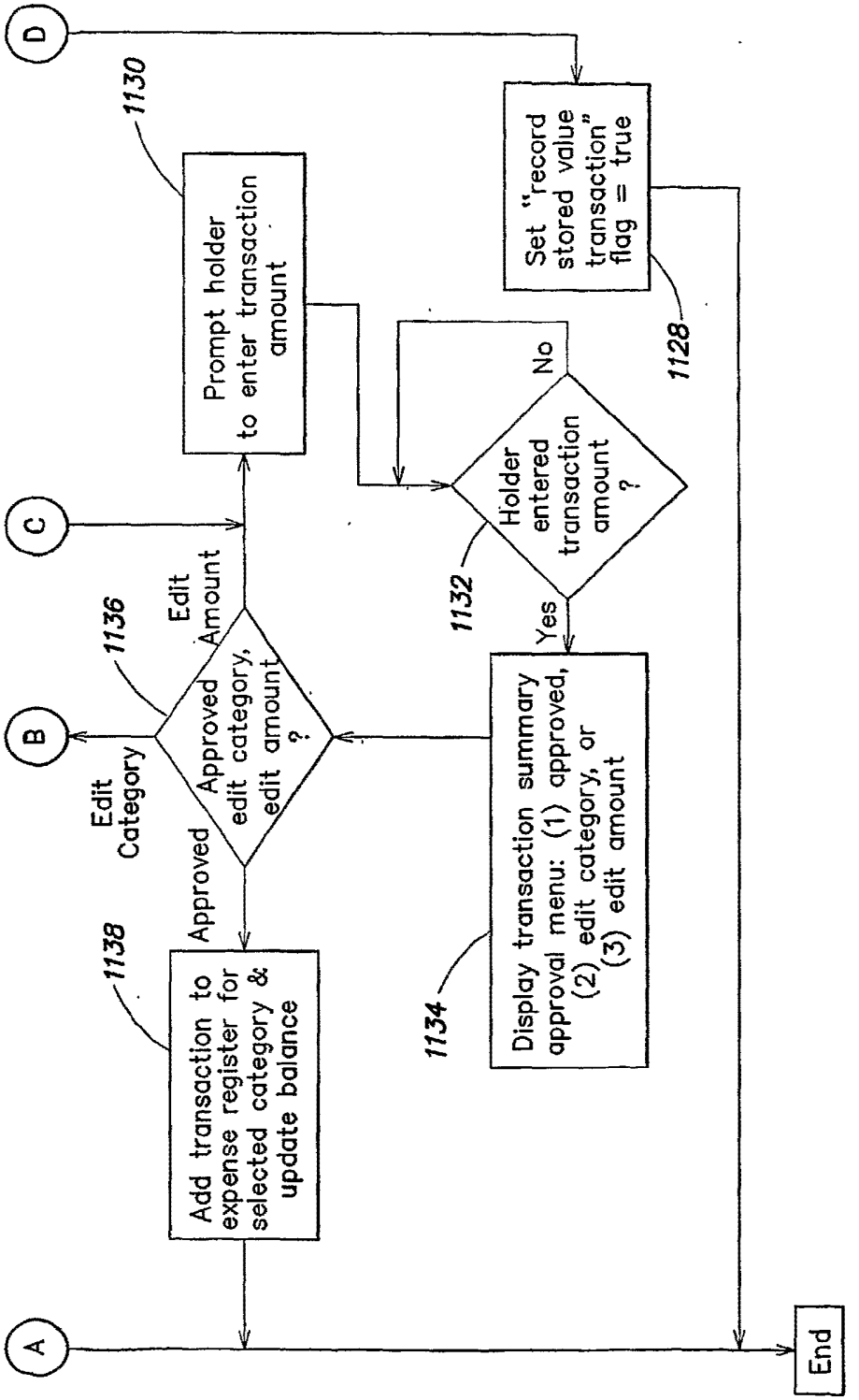

D
1130
Prompt holder to enter transaction amount
Set "record stored value transaction" flag = true
1128
No
Holder entered transaction amount ?
1132
Yes
C
Edit Amount
1136
Approved edit category, edit amount ?
B
Edit Category
Approved
1138
Add transaction to expense register for selected category & update balance
1134
Display transaction summary approval menu: (1) approved, (2) edit category, or (3) edit amount
A
End

FIG. 11B

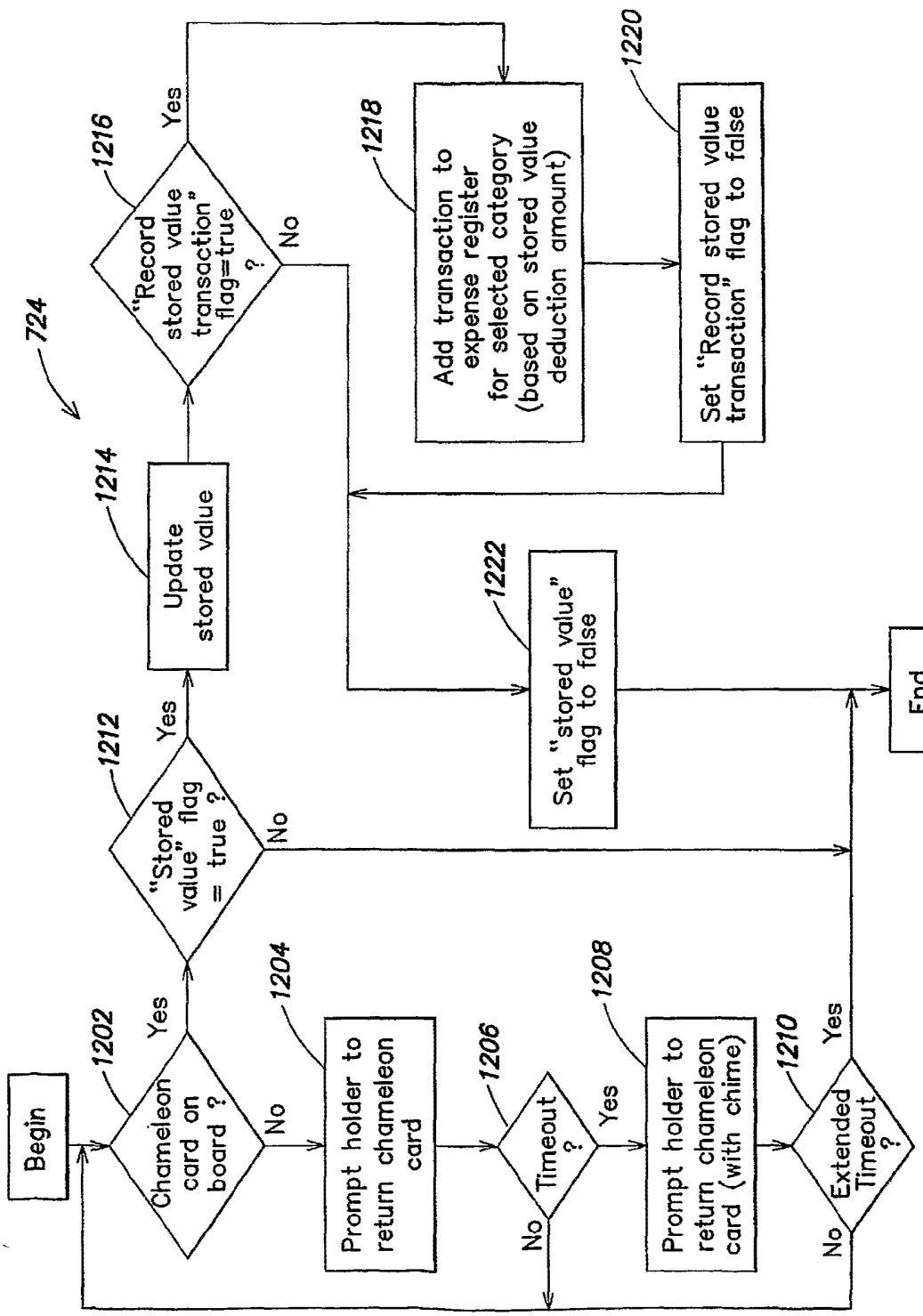

724
Begin
1202
Chameleon card on board ?
Yes
No
1204
Prompt holder to return chameleon card
1206
Timeout ?
No
Yes
1208
Prompt holder to return chameleon card (with chime)
1210
Extended Timeout ?
No
Yes
1212
"Stored value" flag = true ?
Yes
No
1214
Update stored value
1216
"Record stored value transaction" flag=true ?
Yes
No
1218
Add transaction to expense register for selected category (based on stored value deduction amount)
1220
Set "Record stored value transaction" flag to false
1222
Set "stored value" flag to false
End

FIG. 12

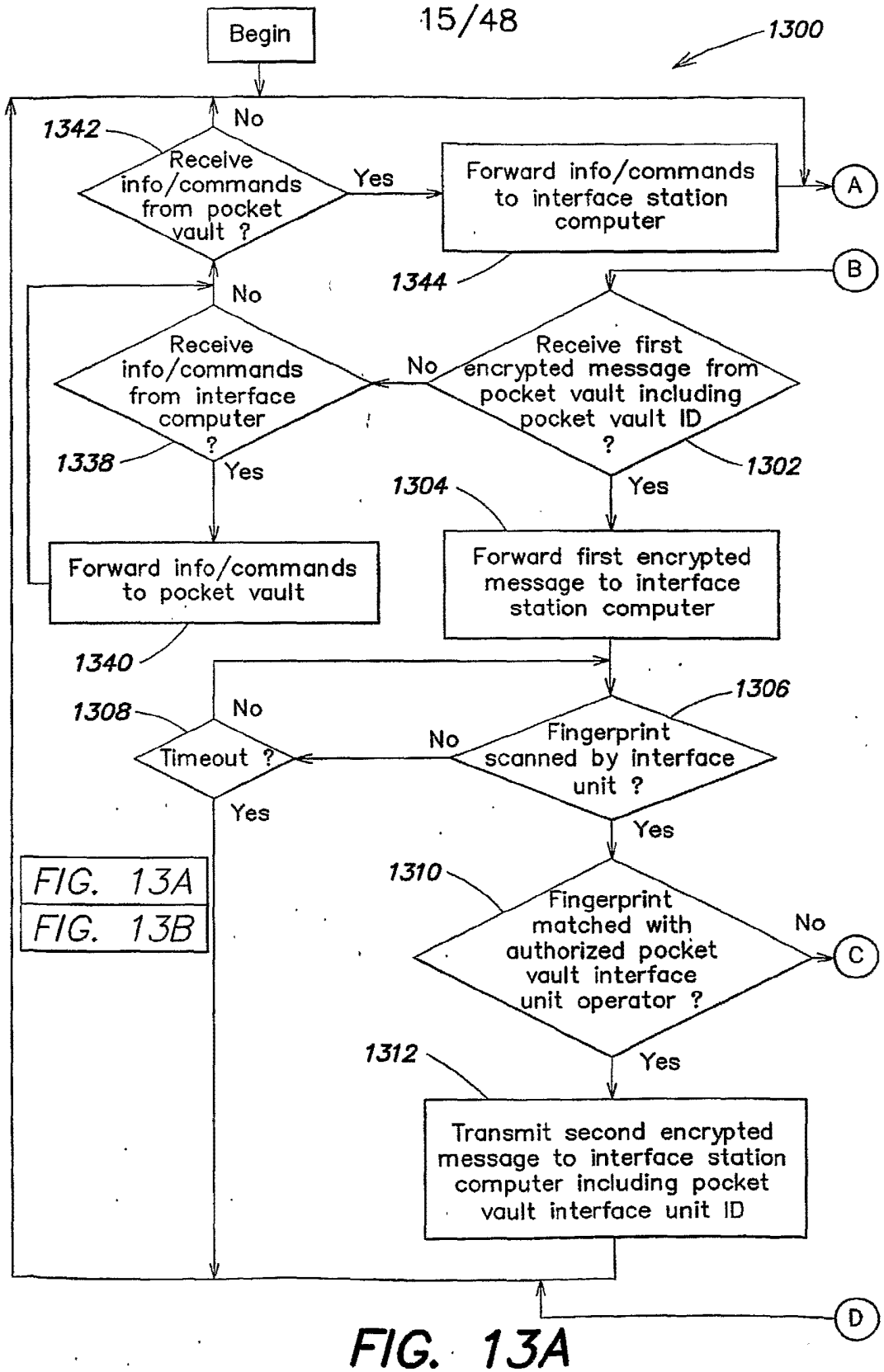


FIG. 13A
FIG. 13B

FIG. 13A

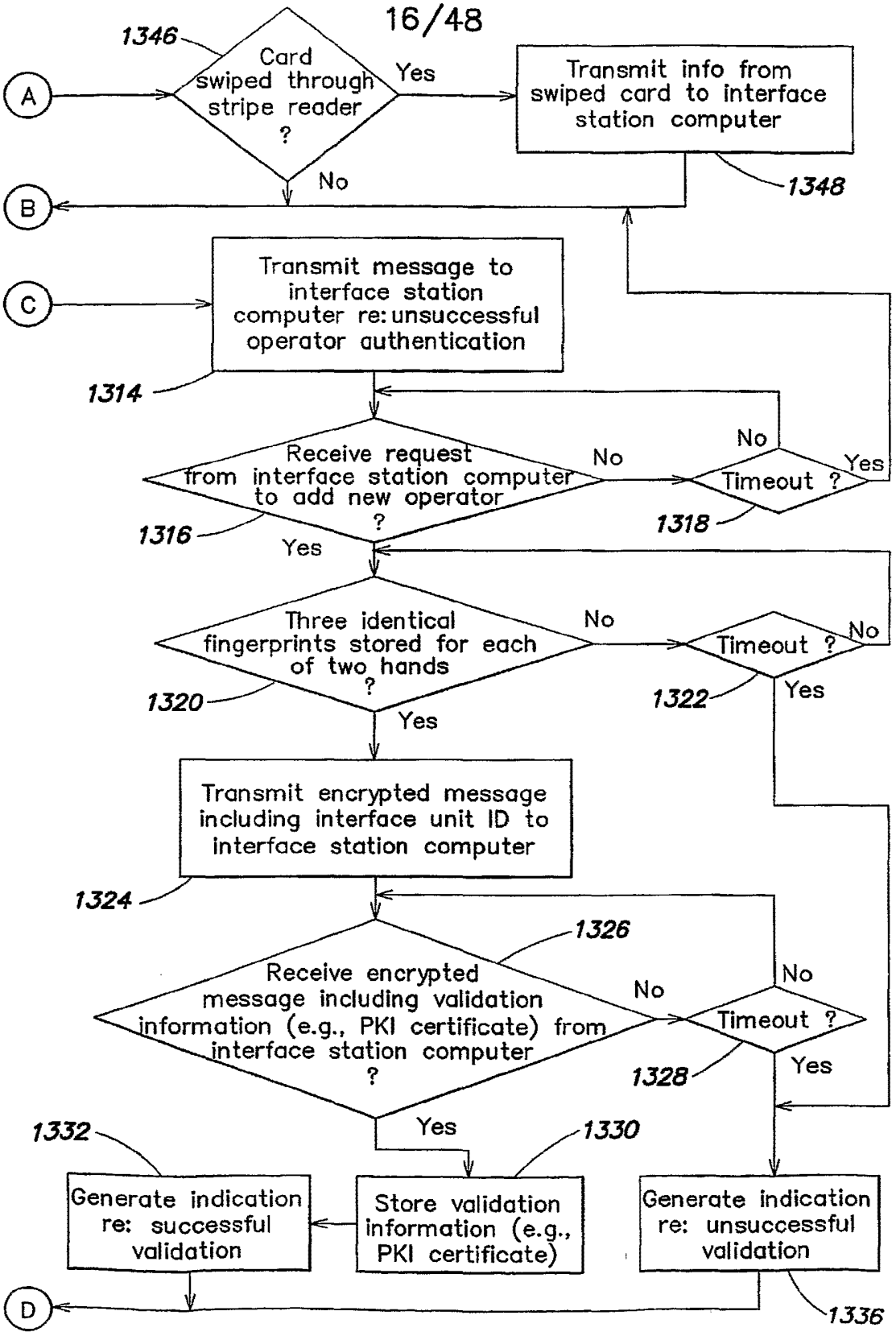

1346
Card swiped through stripe reader ?
Yes
No
A
B
Transmit info from swiped card to interface station computer
1348
C
Transmit message to interface station computer re: unsuccessful operator authentication
1314
Receive request from interface station computer to add new operator ?
1316
No
Yes
Timeout ?
1318
No
Yes
Three identical fingerprints stored for each of two hands ?
1320
No
Yes
Timeout ?
1322
No
Yes
Transmit encrypted message including interface unit ID to interface station computer
1324
1326
Receive encrypted message including validation information (e.g., PKI certificate) from interface station computer ?
No
Yes
Timeout ?
1328
No
Yes
1332
1330
Generate indication re: successful validation
Store validation information (e.g., PKI certificate)
Generate indication re: unsuccessful validation
1336
D

FIG. 13B

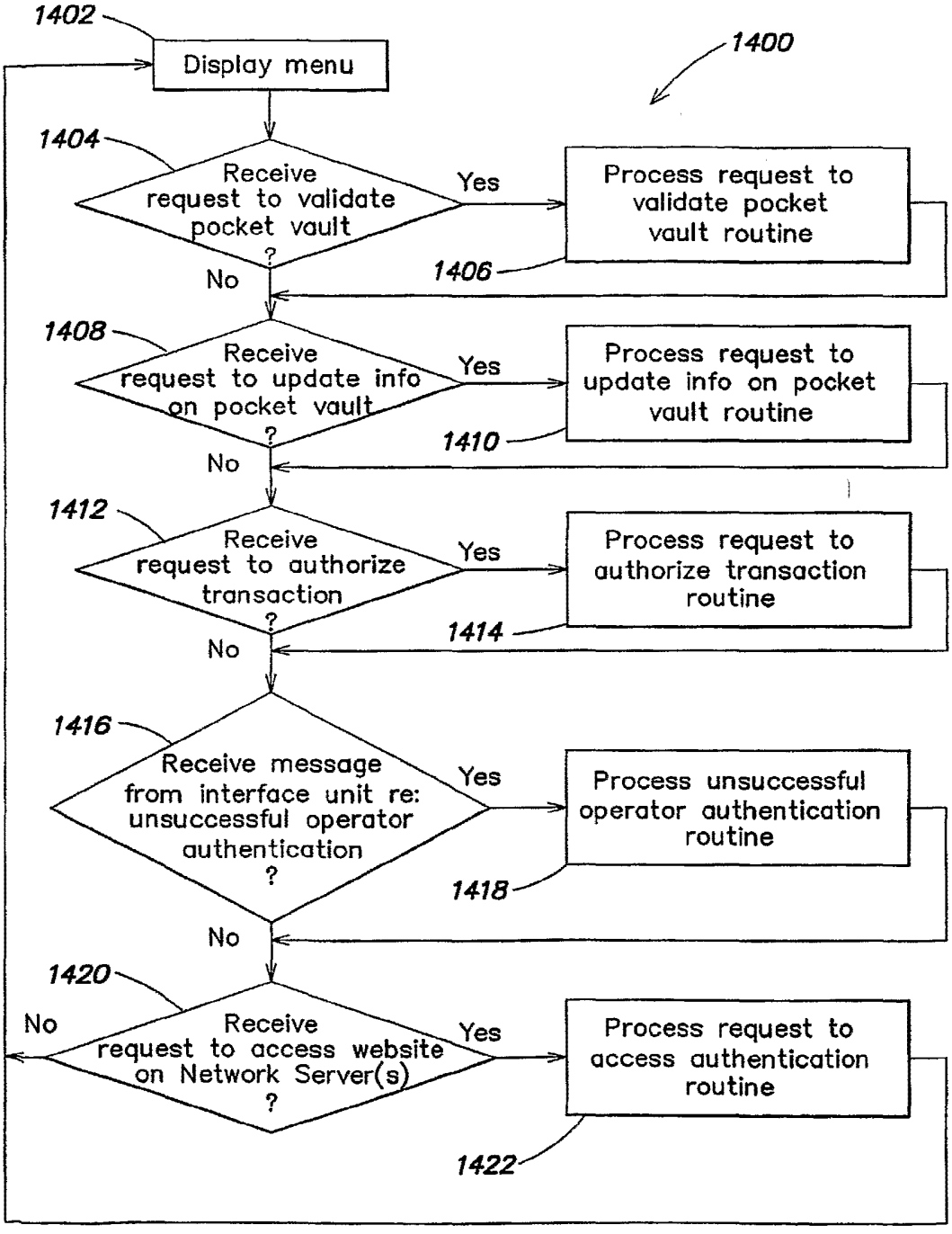

1402
Display menu
1400
1404
Receive request to validate pocket vault ?
Yes
Process request to validate pocket vault routine
1406
No
1408
Receive request to update info on pocket vault ?
Yes
Process request to update info on pocket vault routine
1410
No
1412
Receive request to authorize transaction ?
Yes
Process request to authorize transaction routine
1414
No
1416
Receive message from interface unit re: unsuccessful operator authentication ?
Yes
Process unsuccessful operator authentication routine
1418
No
1420
No
Receive request to access website on Network Server(s) ?
Yes
Process request to access authentication routine
1422

FIG. 14

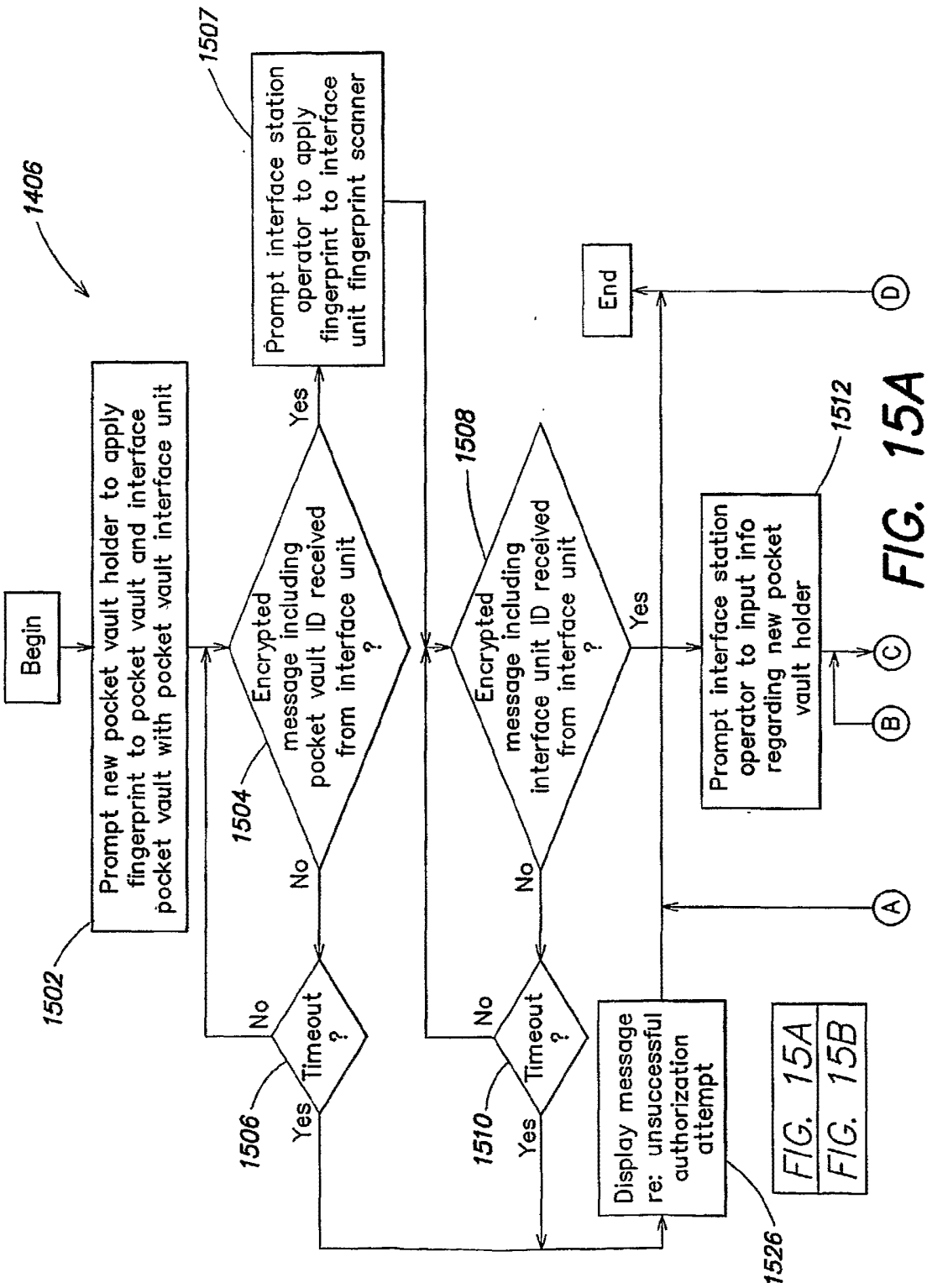


FIG. 15A

FIG. 15A
FIG. 15B

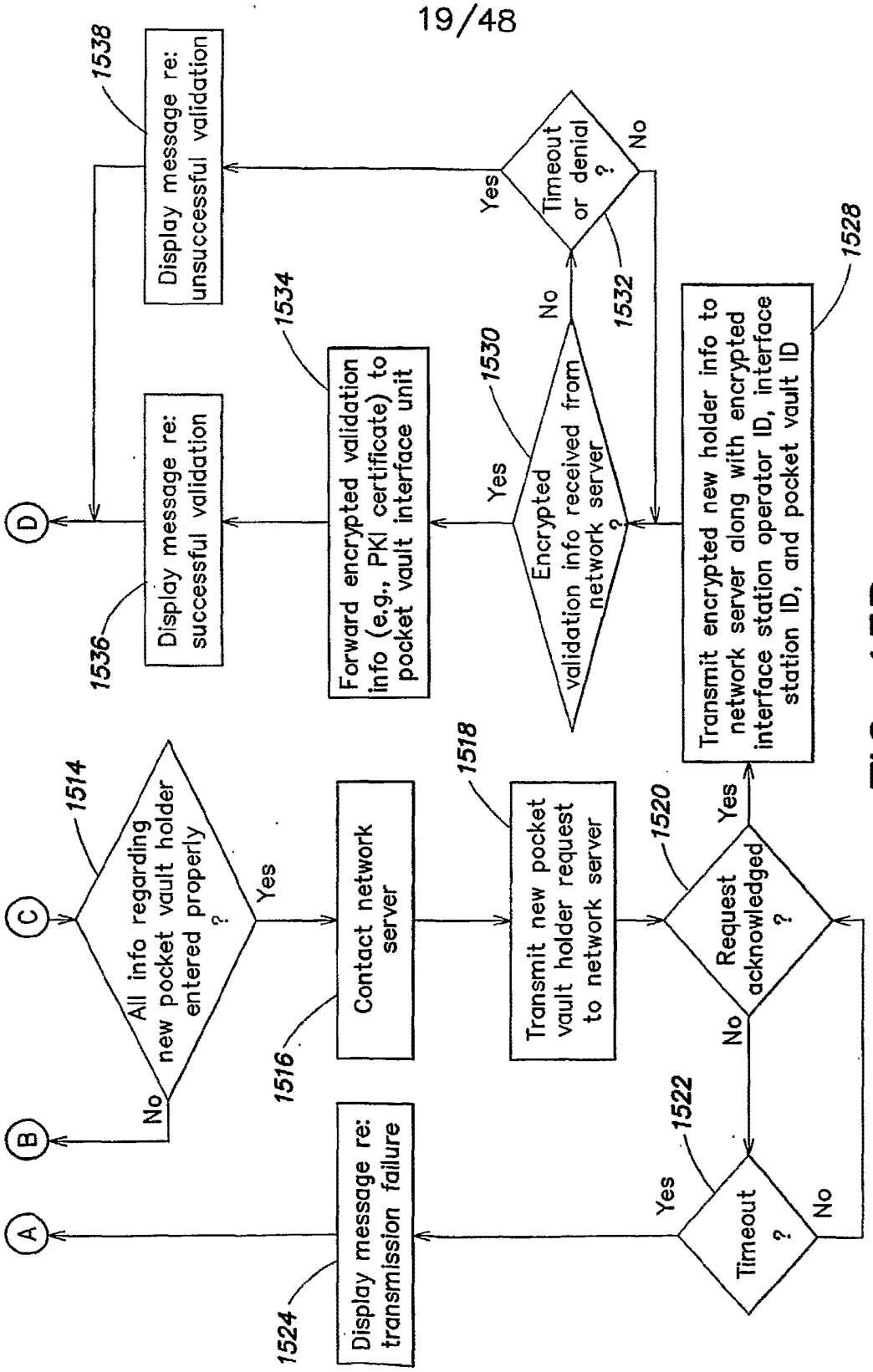

A
B
C
D
All info regarding new pocket vault holder entered properly ?
1514
No
Yes
Contact network server
1516
Transmit new pocket vault holder request to network server
1518
Request acknowledged ?
1520
No
Yes
Timeout ?
1522
Yes
No
Display message re: transmission failure
1524
Transmit encrypted new holder info to network server along with encrypted interface station operator ID, interface station ID, and pocket vault ID
1528
Encrypted validation info received from network server ?
1530
No
Yes
Timeout or denial ?
1532
Yes
No
Forward encrypted validation info (e.g., PKI certificate) to pocket vault interface unit
1534
Display message re: successful validation
1536
Display message re: unsuccessful validation
1538

FIG. 15B

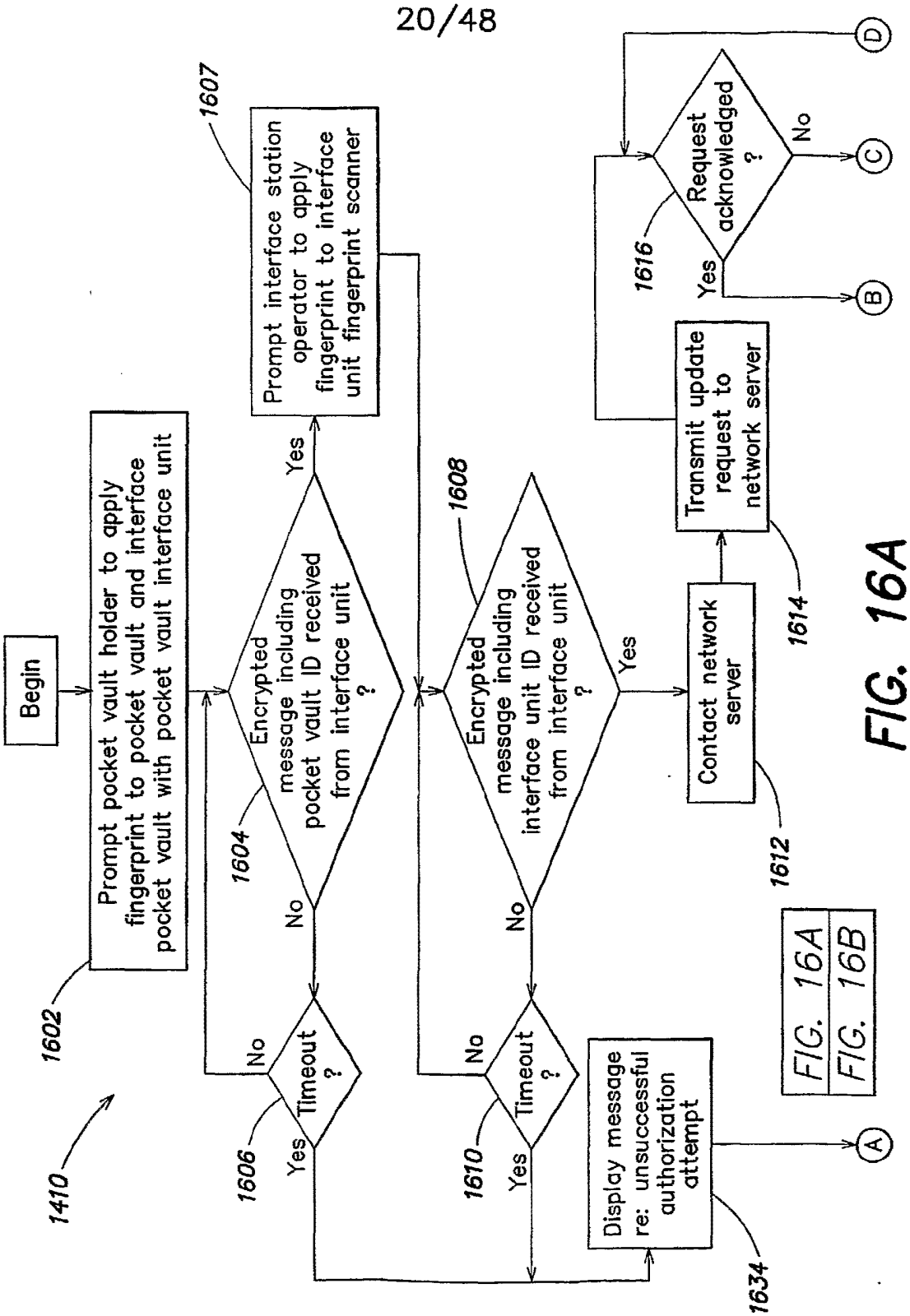


FIG. 16A

FIG. 16A
FIG. 16B

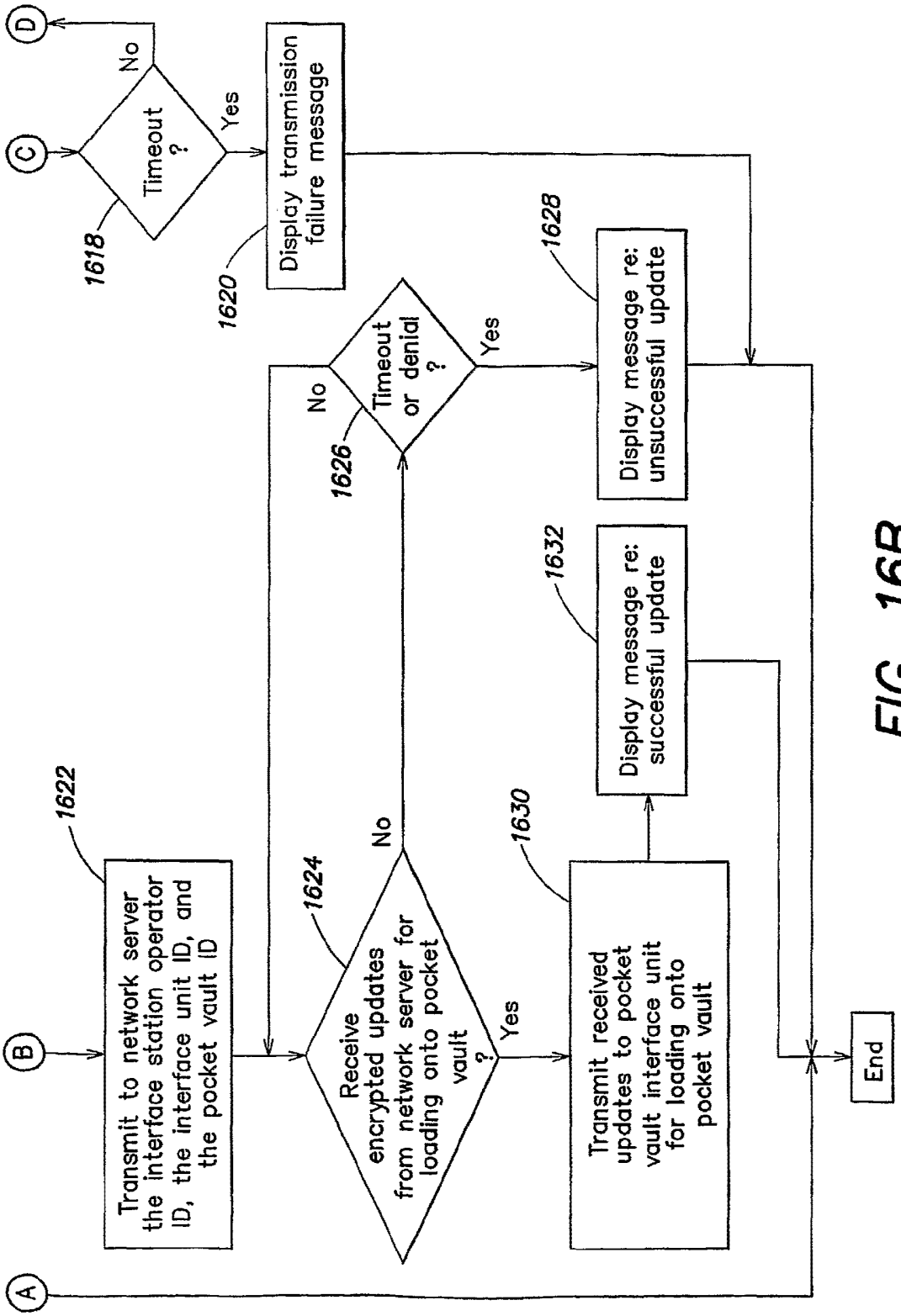

A
B
C
D
Transmit to network server the interface station operator ID, the interface unit ID, and the pocket vault ID
1622
Receive encrypted updates from network server for loading onto pocket vault ?
1624
No
Yes
Timeout or denial ?
1626
No
Yes
Timeout ?
1618
No
Yes
Display transmission failure message
1620
Display message re: unsuccessful update
1628
Display message re: successful update
1632
Transmit received updates to pocket vault interface unit for loading onto pocket vault
1630
End

FIG. 16B

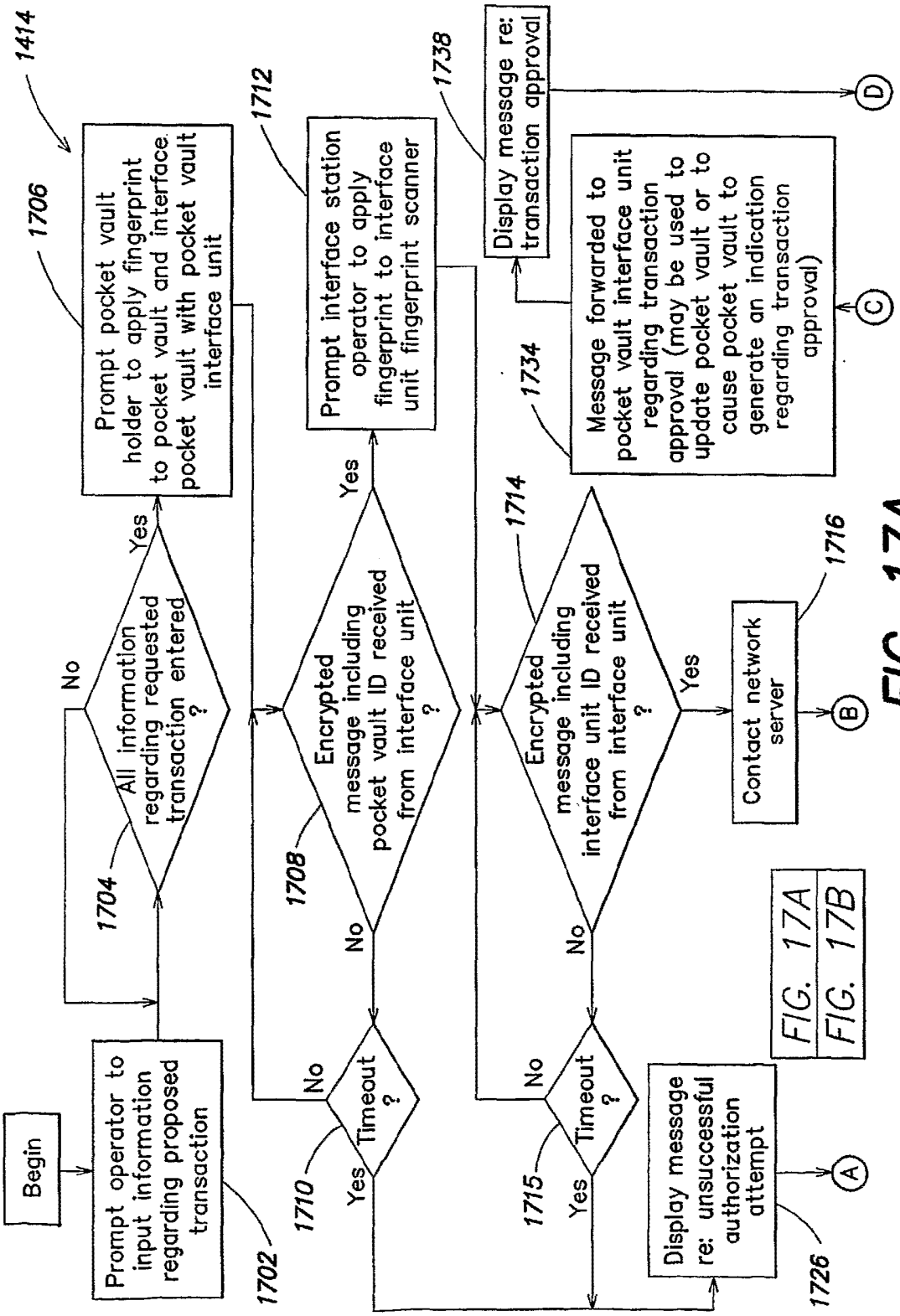


FIG. 17A

FIG. 17A
FIG. 17B

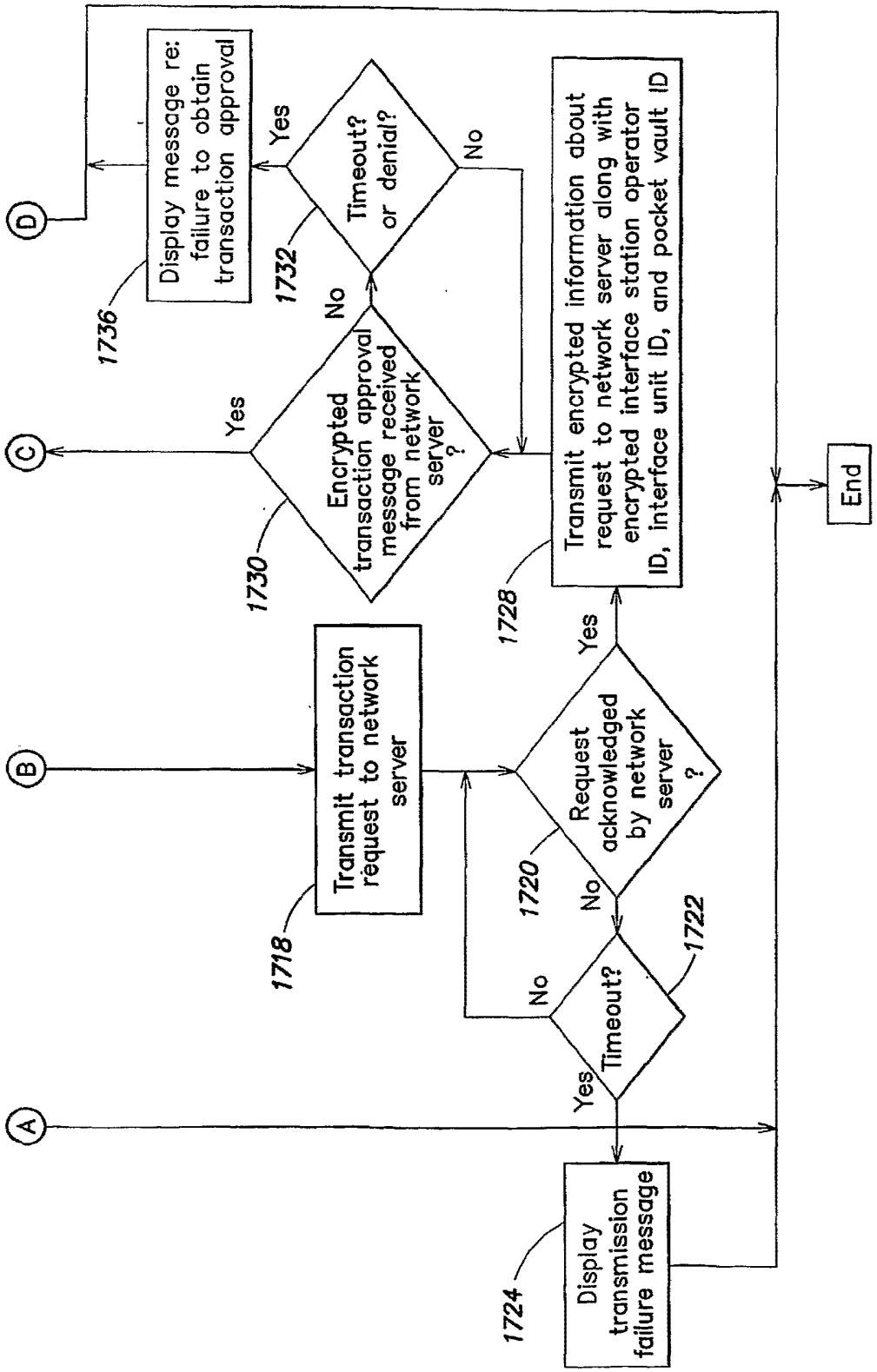

A
B
C
D
Transmit transaction request to network server
1718
Request acknowledged by network server ?
1720
Yes
No
Timeout?
1722
No
Yes
Display transmission failure message
1724
Transmit encrypted information about request to network server along with encrypted interface station operator ID, interface unit ID, and pocket vault ID
1728
Encrypted transaction approval message received from network server ?
1730
Yes
No
Timeout? or denial?
1732
Yes
No
Display message re: failure to obtain transaction approval
1736
End

FIG. 17B

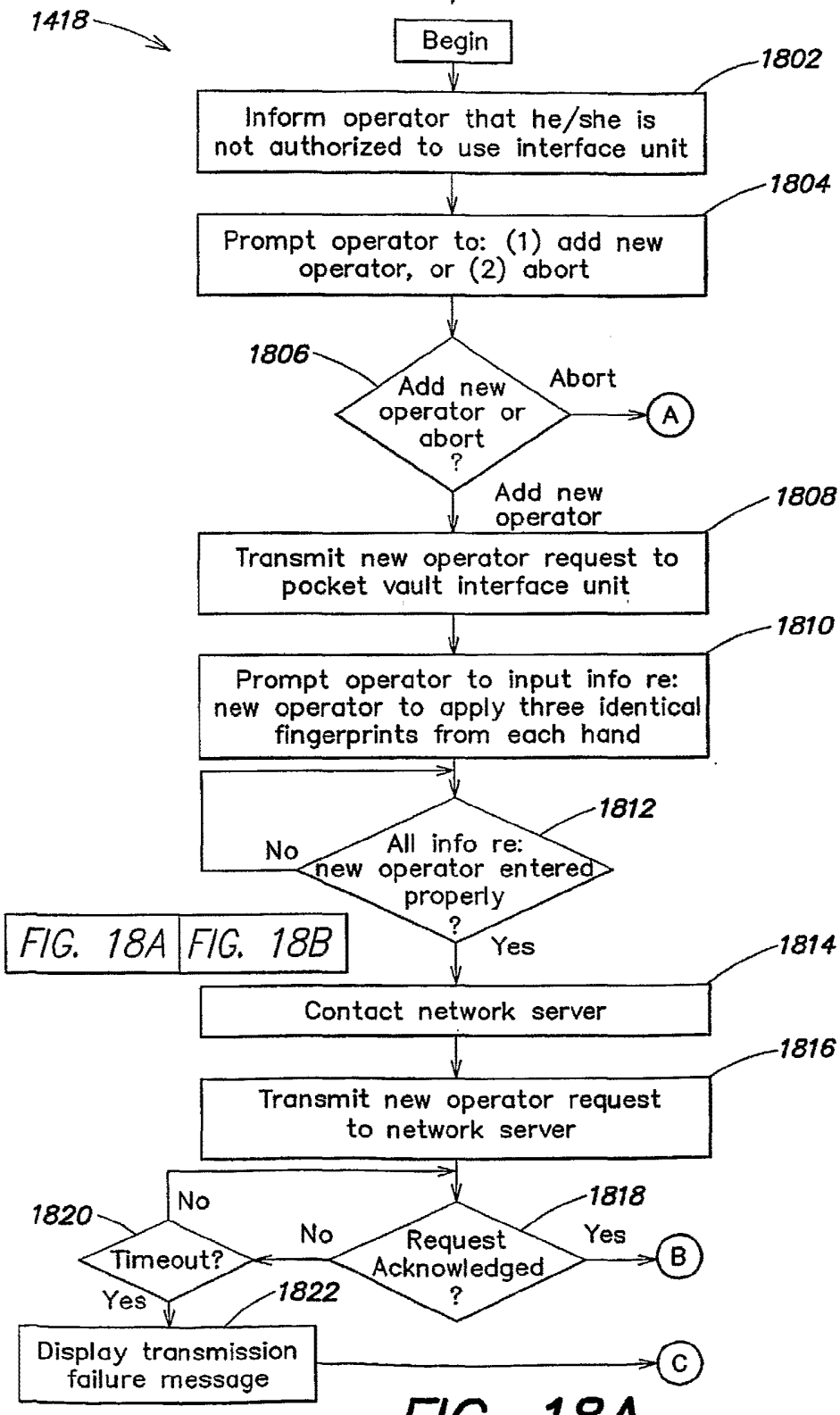


FIG. 18A | FIG. 18B

FIG. 18A

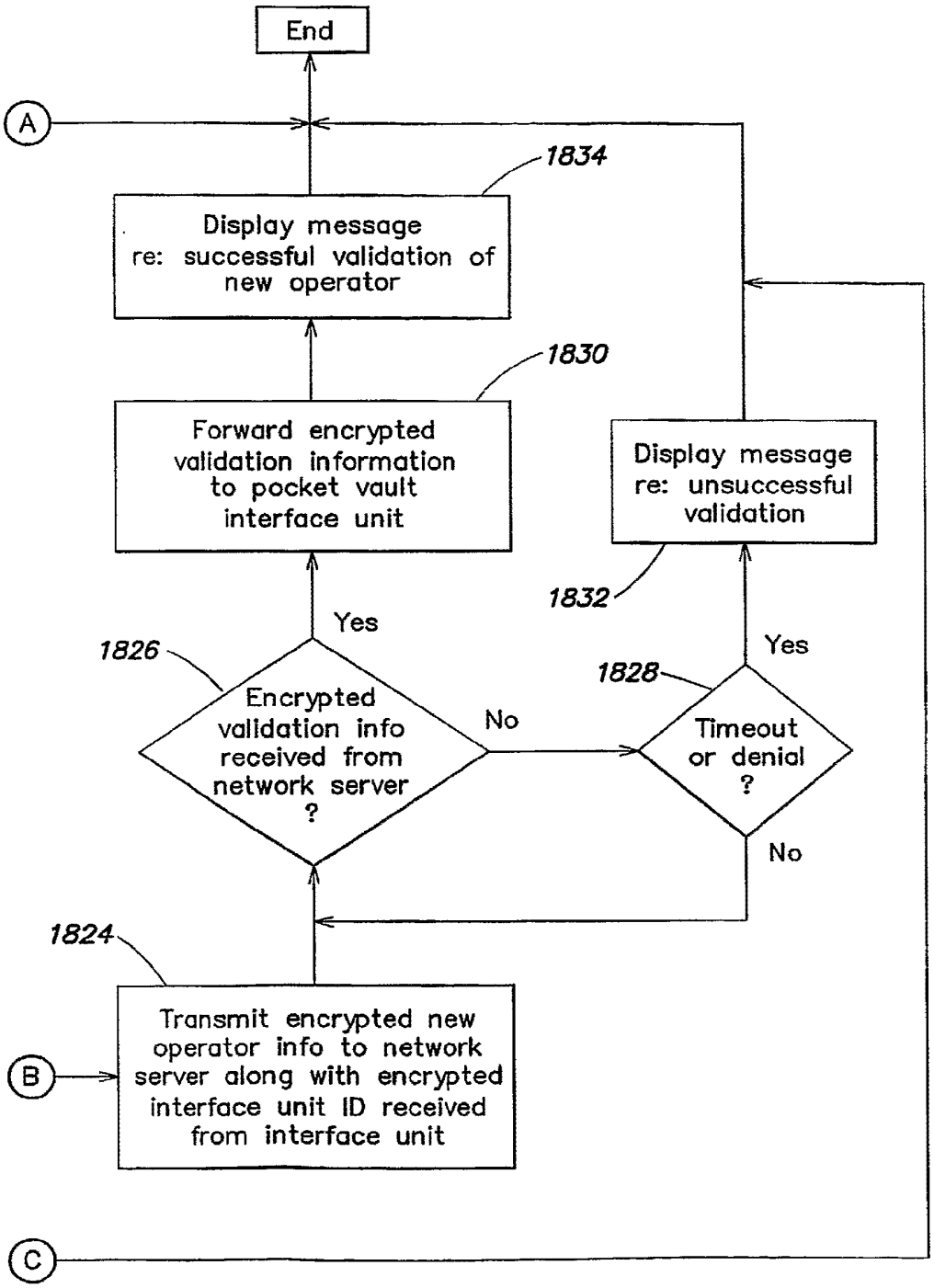

End
A
1834
Display message re: successful validation of new operator
1830
Forward encrypted validation information to pocket vault interface unit
Display message re: unsuccessful validation
1832
Yes
1826
Encrypted validation info received from network server ?
No
1828
Timeout or denial ?
Yes
No
1824
Transmit encrypted new operator info to network server along with encrypted interface unit ID received from interface unit
B
C

FIG. 18B

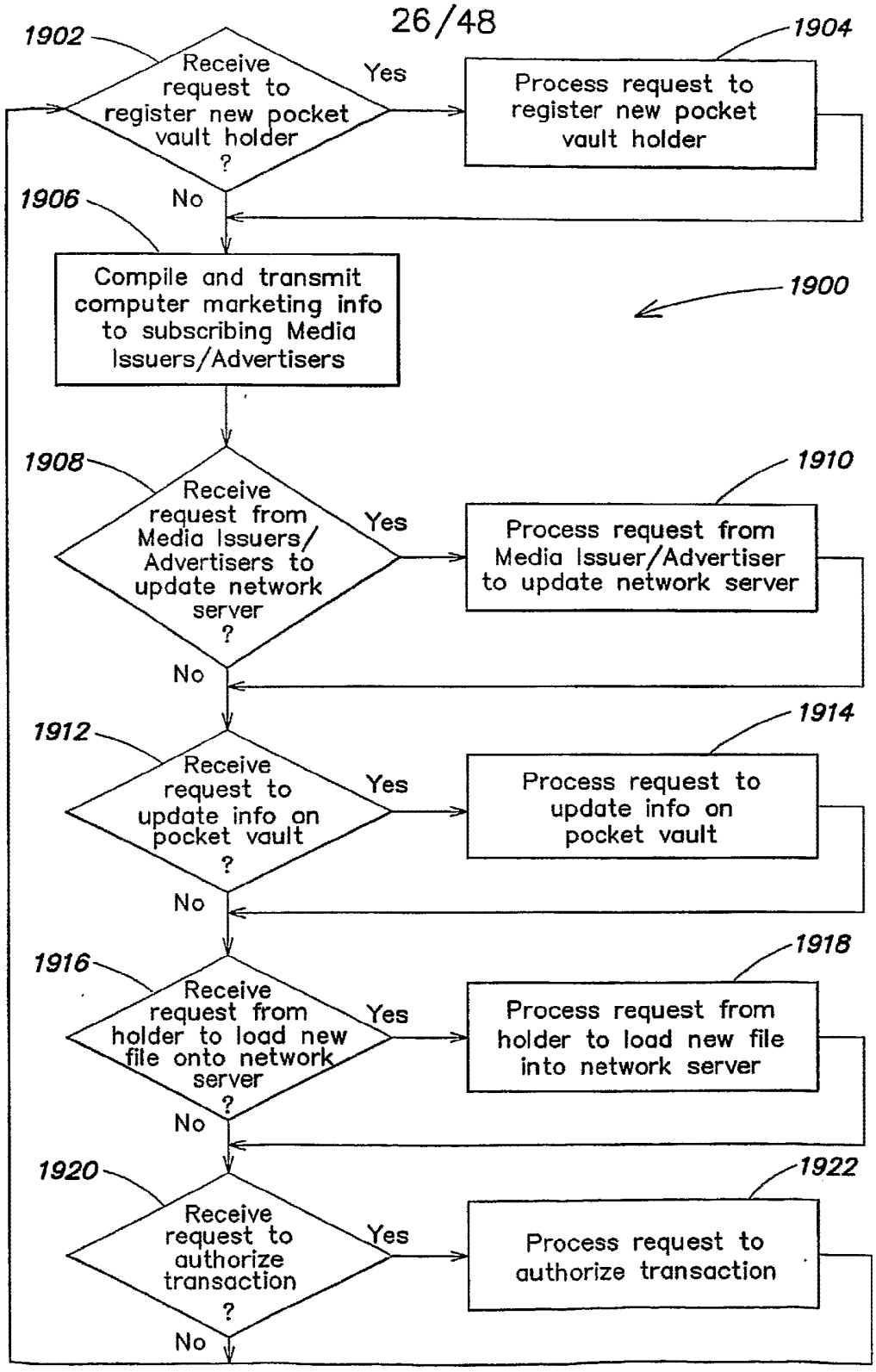

1902
Receive request to register new pocket vault holder ?
Yes
1904
Process request to register new pocket vault holder
No
1906
Compile and transmit computer marketing info to subscribing Media Issuers/Advertisers
1900
1908
Receive request from Media Issuers/ Advertisers to update network server ?
Yes
1910
Process request from Media Issuer/Advertiser to update network server
No
1912
Receive request to update info on pocket vault ?
Yes
1914
Process request to update info on pocket vault
No
1916
Receive request from holder to load new file onto network server ?
Yes
1918
Process request from holder to load new file into network server
No
1920
Receive request to authorize transaction ?
Yes
1922
Process request to authorize transaction
No

FIG. 19

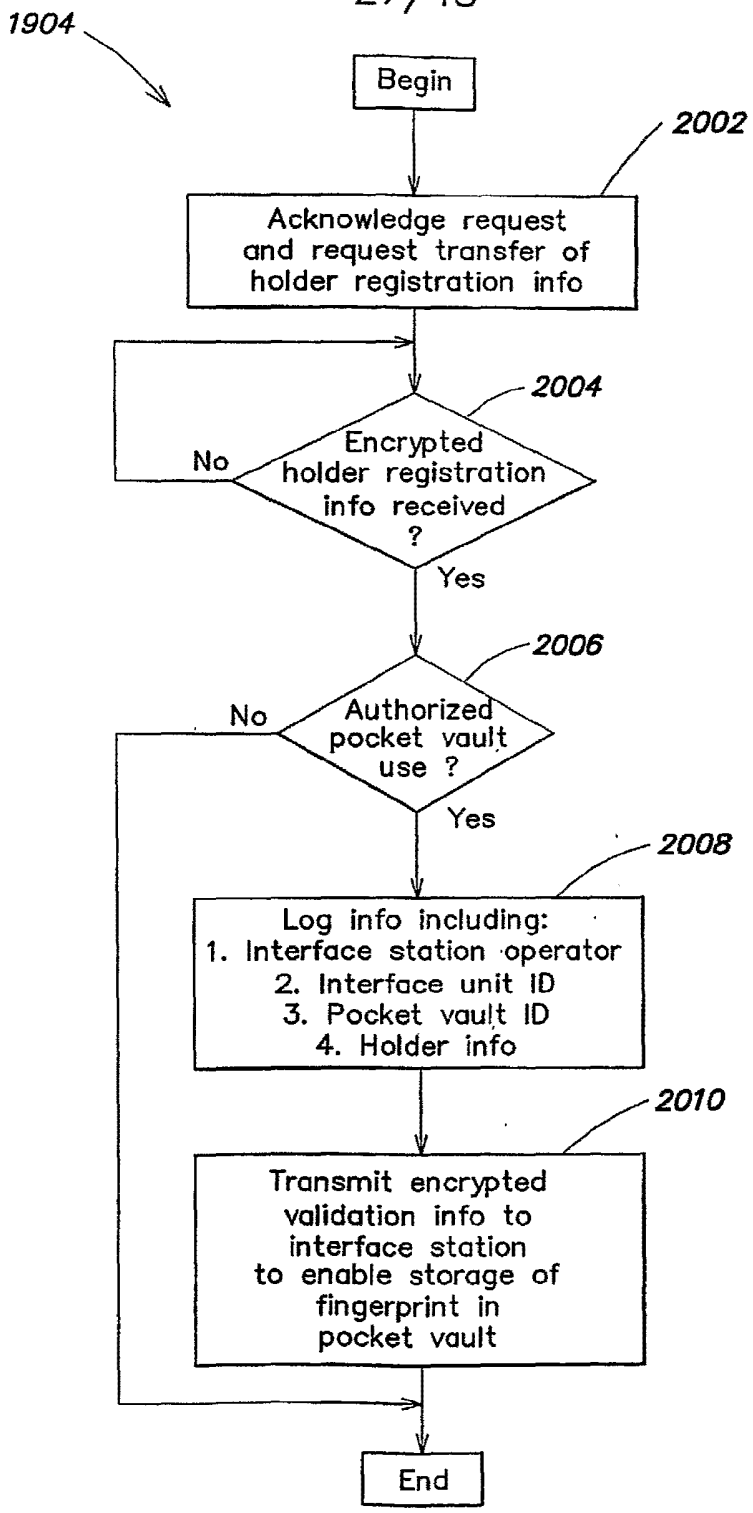

1904
Begin
2002
Acknowledge request and request transfer of holder registration info
2004
Encrypted holder registration info received ?
No
Yes
2006
Authorized pocket vault use ?
No
Yes
2008
Log info including:
1. Interface station operator
2. Interface unit ID
3. Pocket vault ID
4. Holder info
2010
Transmit encrypted validation info to interface station to enable storage of fingerprint in pocket vault
End

FIG. 20

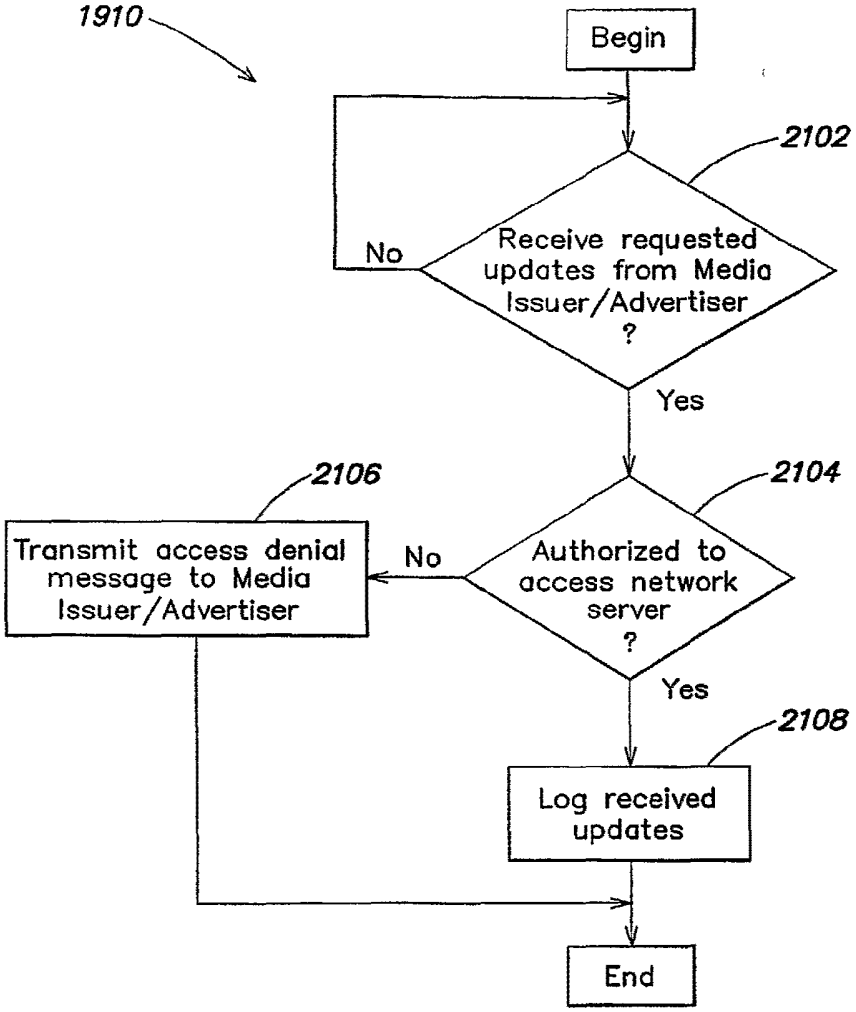

1910
Begin
2102
Receive requested updates from Media Issuer/Advertiser ?
No
Yes
2104
Authorized to access network server ?
No
2106
Transmit access denial message to Media Issuer/Advertiser
Yes
2108
Log received updates
End

FIG. 21

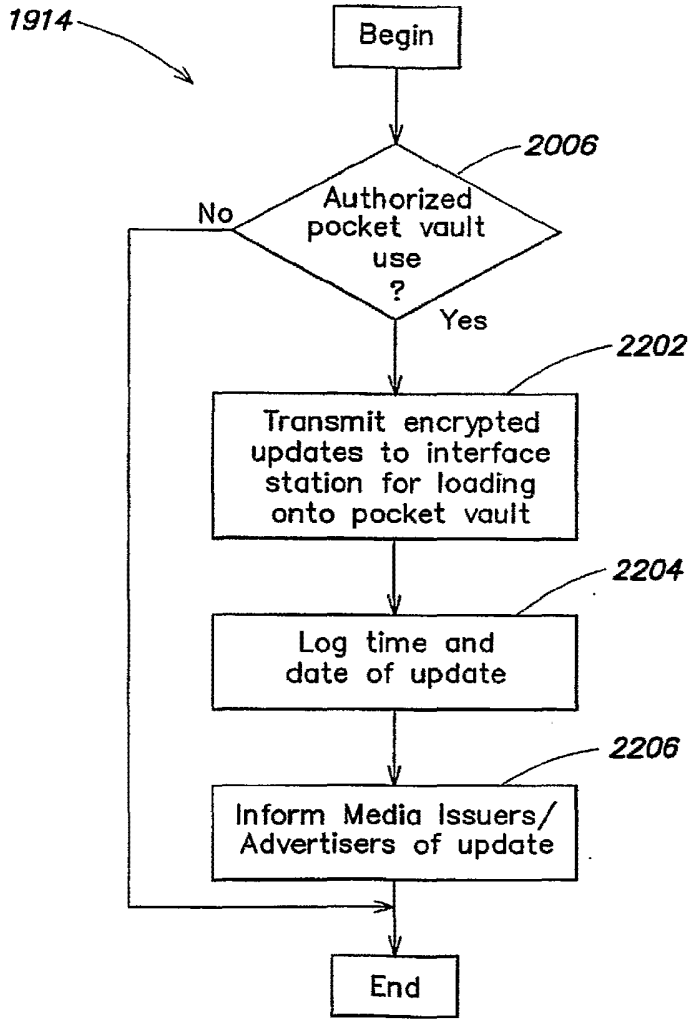

1914
Begin
2006
Authorized pocket vault use ?
No
Yes
2202
Transmit encrypted updates to interface station for loading onto pocket vault
2204
Log time and date of update
2206
Inform Media Issuers/ Advertisers of update
End

FIG. 22

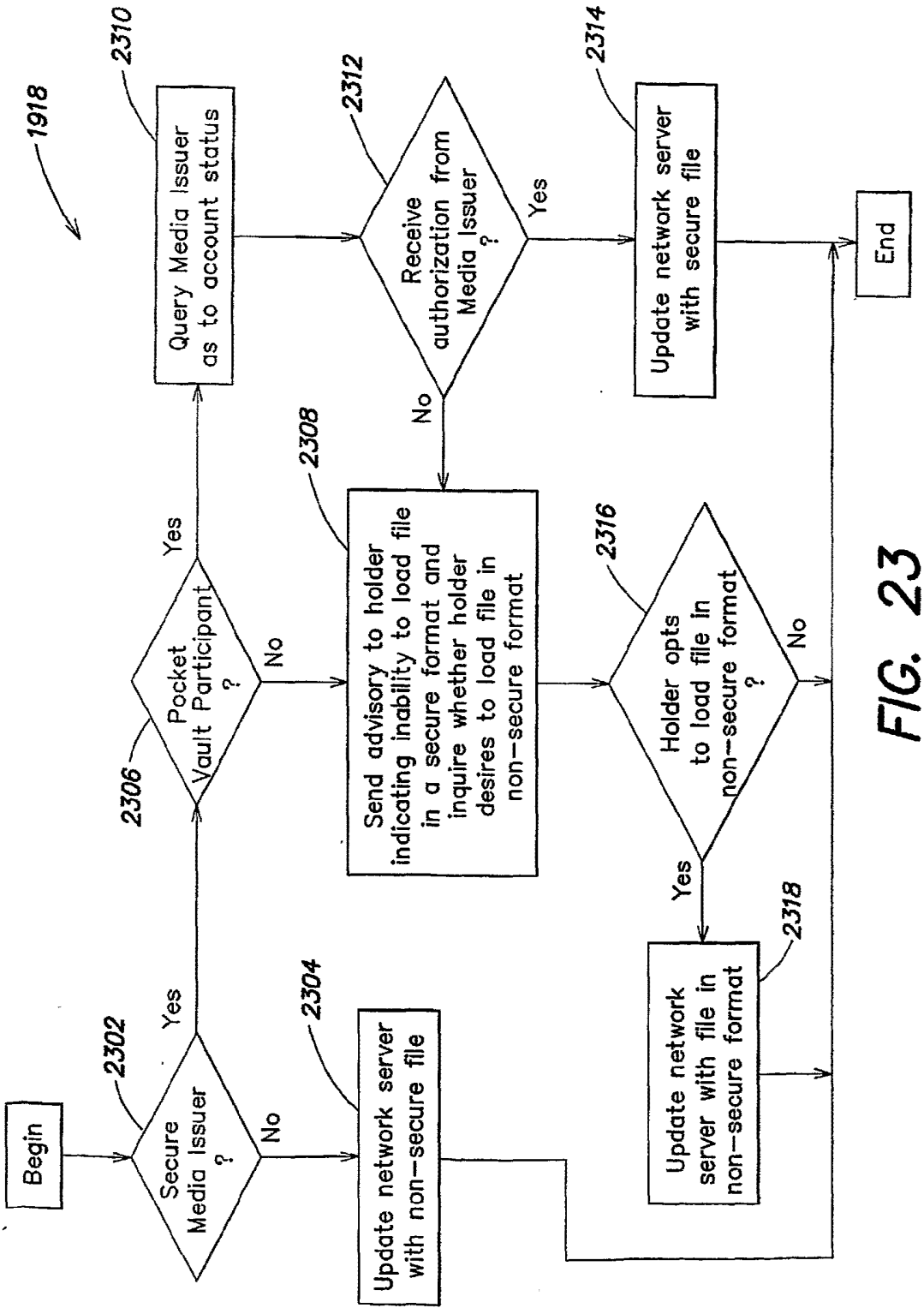

1918
Begin
2302
Secure Media Issuer ?
Yes
No
2304
Update network server with non-secure file
2306
Pocket Vault Participant ?
Yes
No
2308
Send advisory to holder indicating inability to load file in a secure format and inquire whether holder desires to load file in non-secure format
2310
Query Media Issuer as to account status
2312
Receive authorization from Media Issuer ?
Yes
No
2314
Update network server with secure file
2316
Holder opts to load file in non-secure format ?
Yes
No
2318
Update network server with file in non-secure format
End

FIG. 23

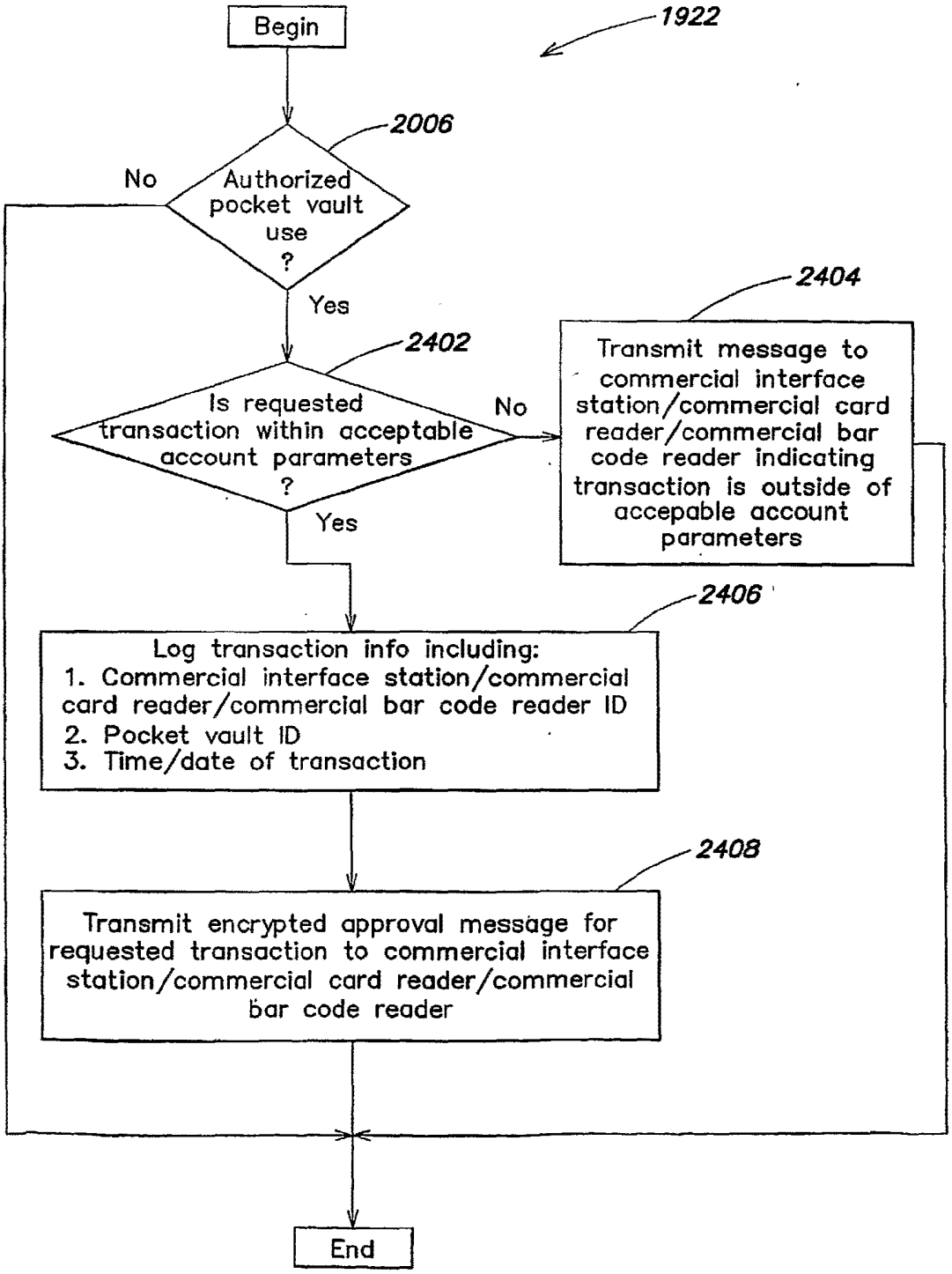

Begin
1922
2006
Authorized pocket vault use ?
No
Yes
2402
Is requested transaction within acceptable account parameters ?
No
Yes
2404
Transmit message to commercial interface station/commercial card reader/commercial bar code reader indicating transaction is outside of accepable account parameters
2406
Log transaction info including:
1. Commercial interface station/commercial card reader/commercial bar code reader ID
2. Pocket vault ID
3. Time/date of transaction
2408
Transmit encrypted approval message for requested transaction to commercial interface station/commercial card reader/commercial bar code reader
End

FIG. 24

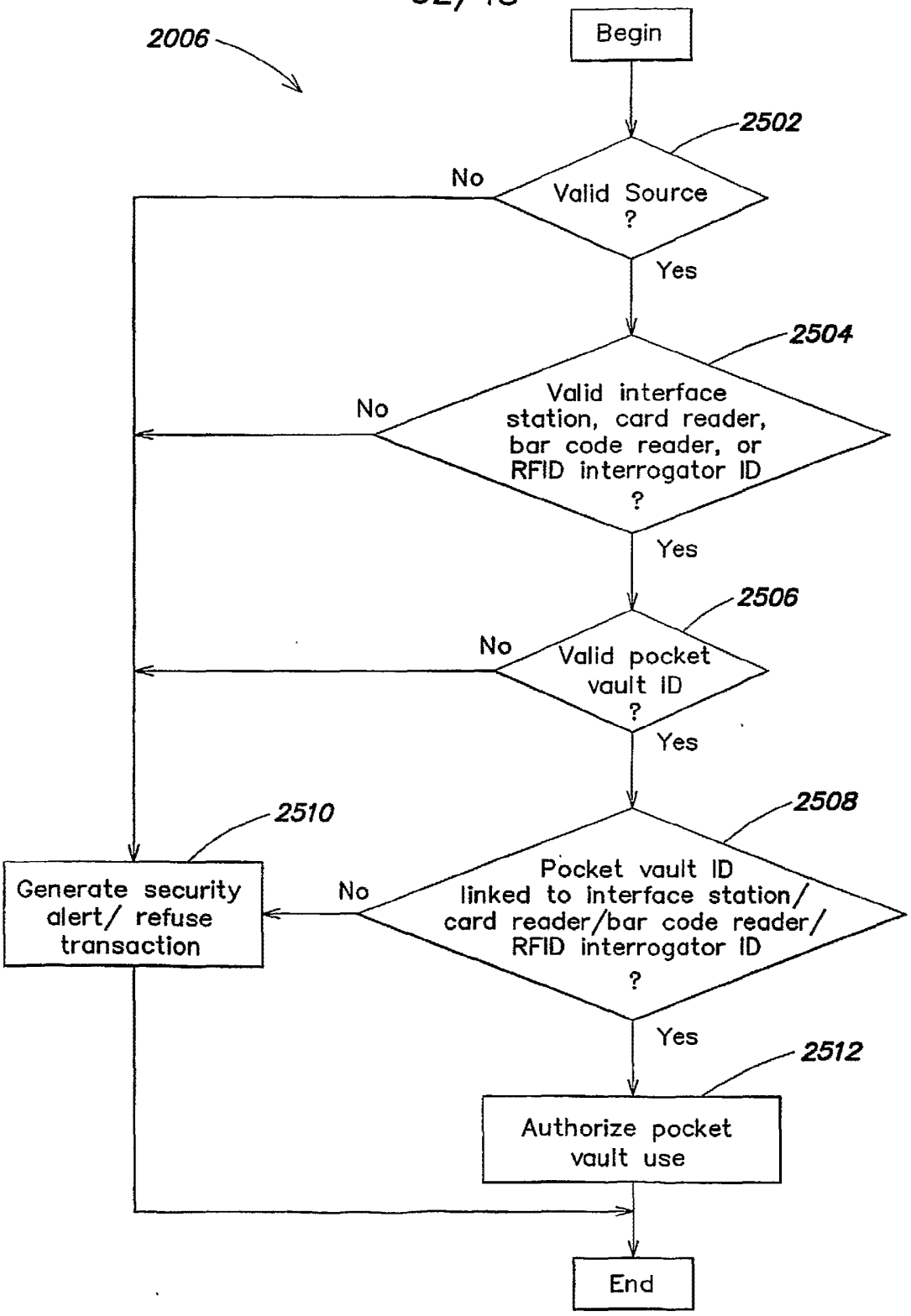

2006
Begin
2502
Valid Source ?
No
Yes
2504
Valid interface station, card reader, bar code reader, or RFID interrogator ID ?
No
Yes
2506
Valid pocket vault ID ?
No
Yes
2508
Pocket vault ID linked to interface station/ card reader/bar code reader/ RFID interrogator ID ?
No
Yes
2510
Generate security alert/ refuse transaction
2512
Authorize pocket vault use
End

FIG. 25

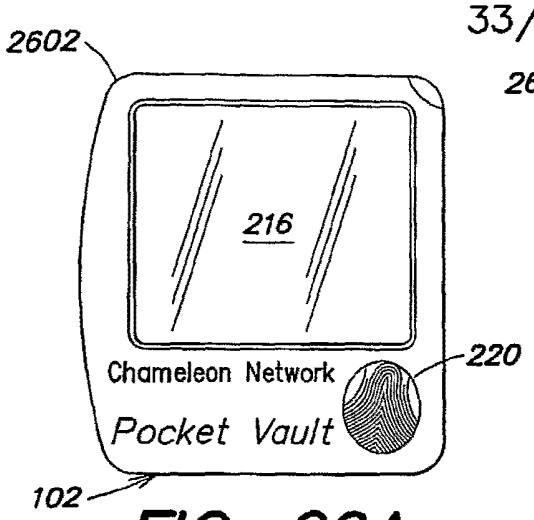


FIG. 26A

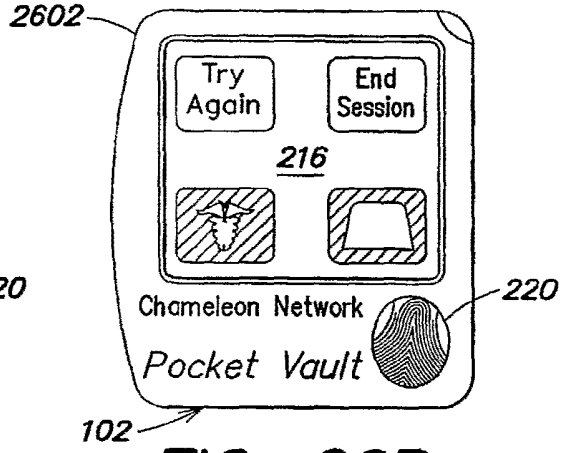


FIG. 26B

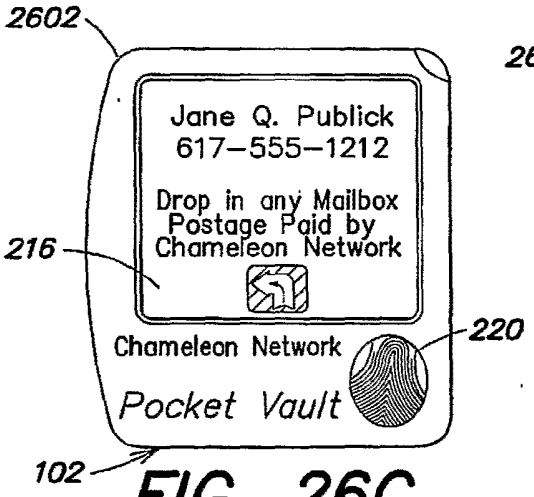


FIG. 26C

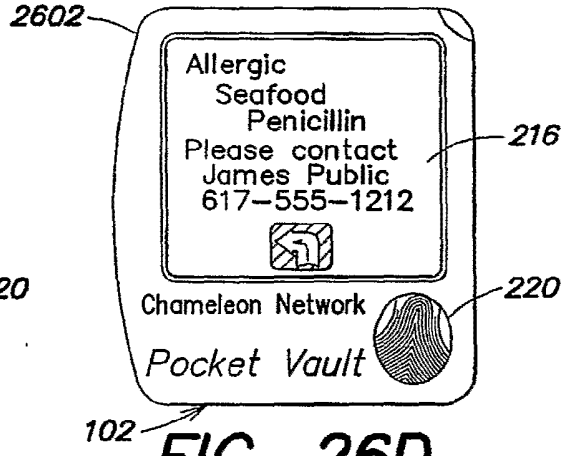


FIG. 26D

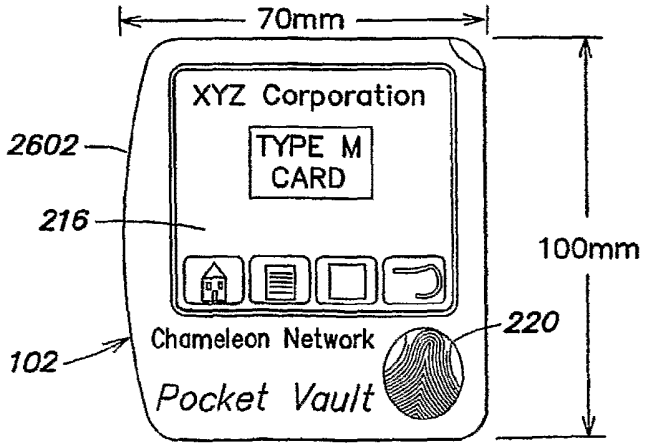


FIG. 26E

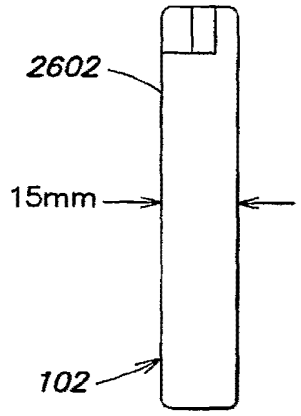


FIG. 26F

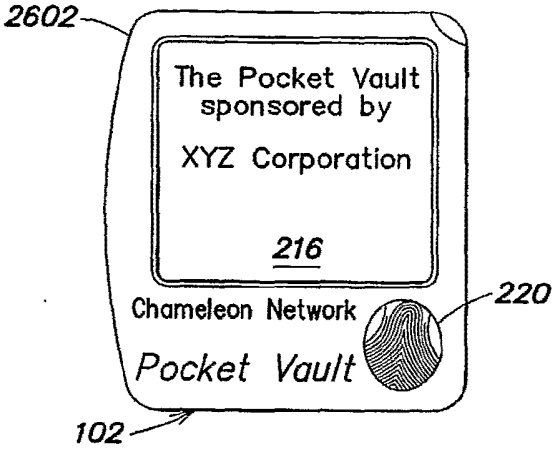


FIG. 26G

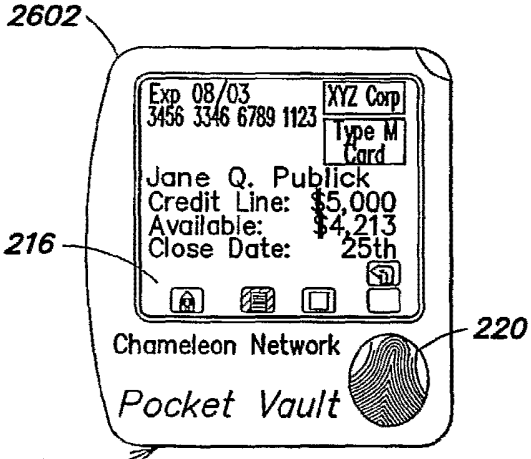


FIG. 26H

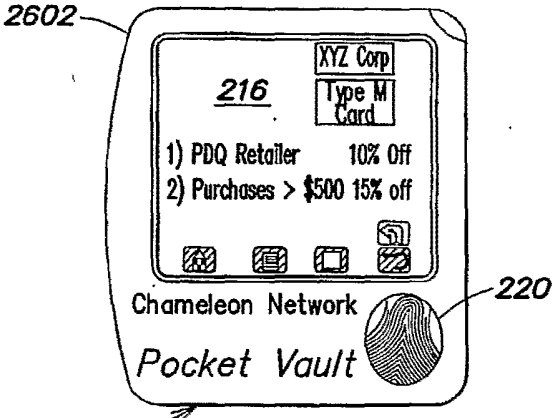


FIG. 26I

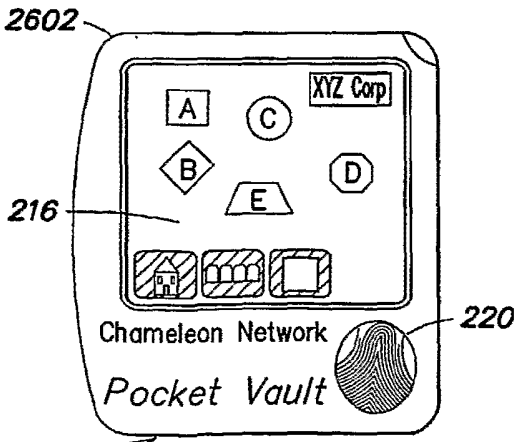


FIG. 26J

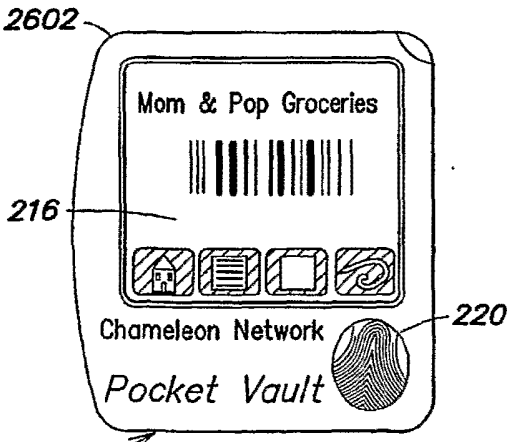


FIG. 26K

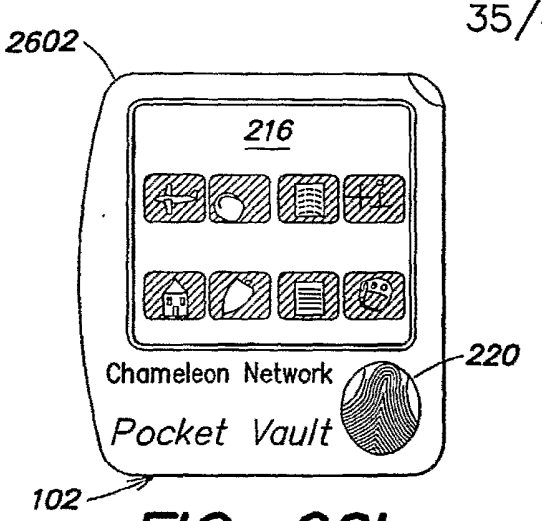


FIG. 26L

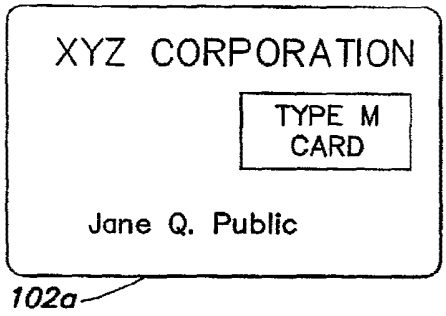


FIG. 26M

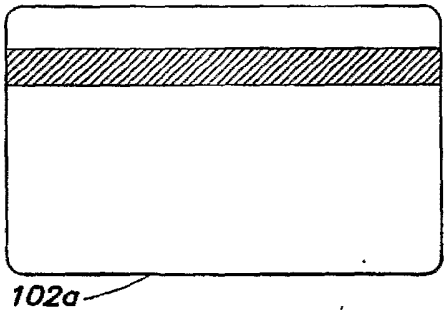


FIG. 26N

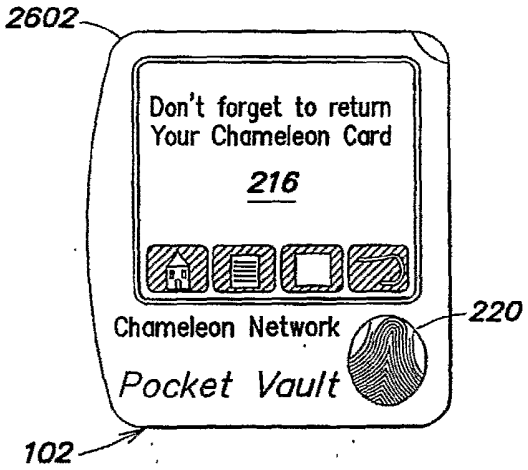


FIG. 26O

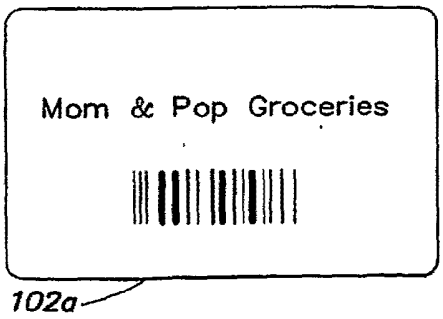


FIG. 26P

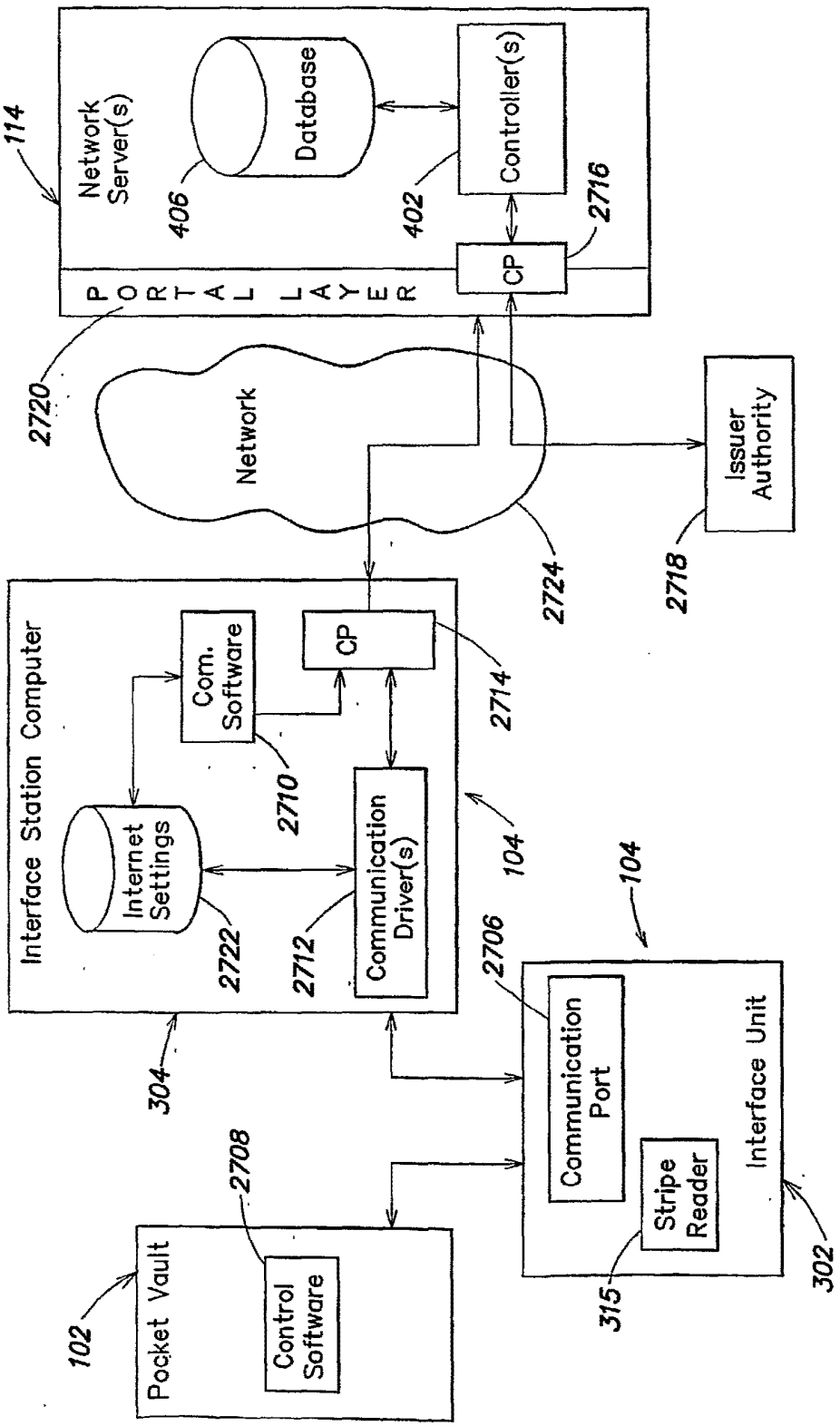

114
Network Server(s)
Database
406
Controller(s)
402
2716
PORTAL LAYER
CP
2720
Network
Issuer Authority
2724
2718
Interface Station Computer
Com. Software
CP
2714
2710
Internet Settings
Communication Driver(s)
104
2722
2712
2706
104
Communication Port
Stripe Reader
Interface Unit
304
315
302
2708
Pocket Vault
Control Software
102

FIG. 27

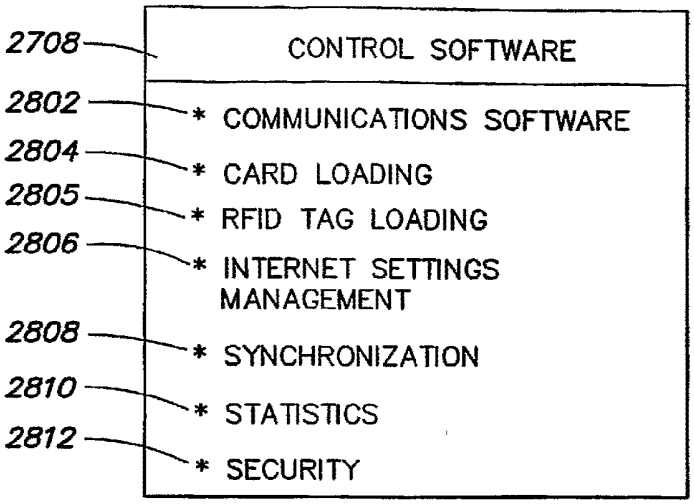

2708
CONTROL SOFTWARE
2802
* COMMUNICATIONS SOFTWARE
2804
* CARD LOADING
2805
* RFID TAG LOADING
2806
* INTERNET SETTINGS MANAGEMENT
2808
* SYNCHRONIZATION
2810
* STATISTICS
2812
* SECURITY

FIG. 28

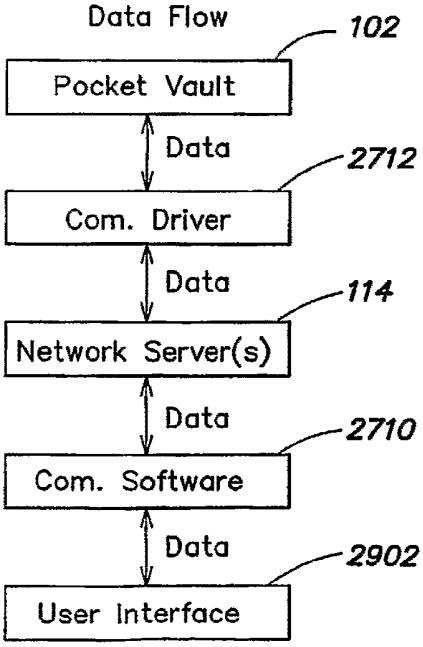

Data Flow
102
Pocket Vault
Data
2712
Com. Driver
Data
114
Network Server(s)
Data
2710
Com. Software
Data
2902
User Interface

FIG. 29

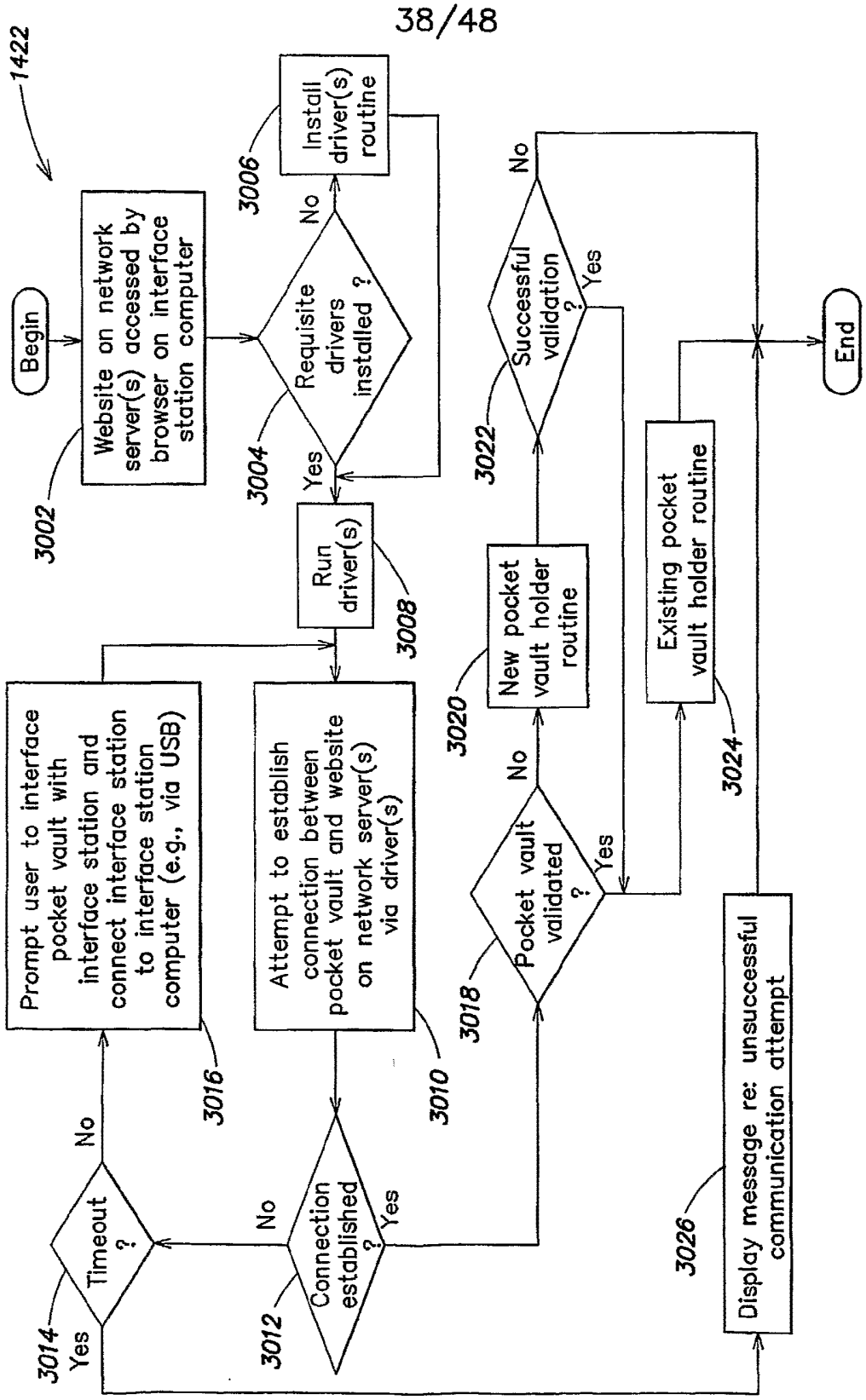

1422
Begin
Website on network server(s) accessed by browser on interface station computer
3002
Requisite drivers installed ?
3004
No
Yes
Install driver(s) routine
3006
Run driver(s)
3008
Prompt user to interface pocket vault with interface station and connect interface station to interface station computer (e.g., via USB)
3016
Attempt to establish connection between pocket vault and website on network server(s) via driver(s)
3010
Timeout ?
3014
Connection established ?
3012
Pocket vault validated ?
3018
New pocket vault holder routine
3020
Successful validation ?
3022
Existing pocket vault holder routine
3024
Display message re: unsuccessful communication attempt
3026
End

FIG. 30

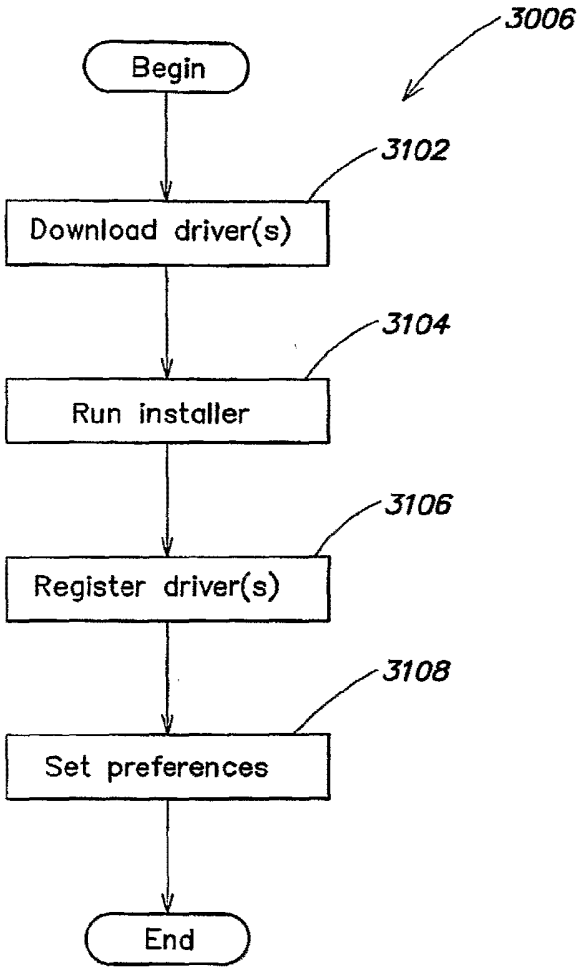

3006
Begin
3102
Download driver(s)
3104
Run installer
3106
Register driver(s)
3108
Set preferences
End

FIG. 31

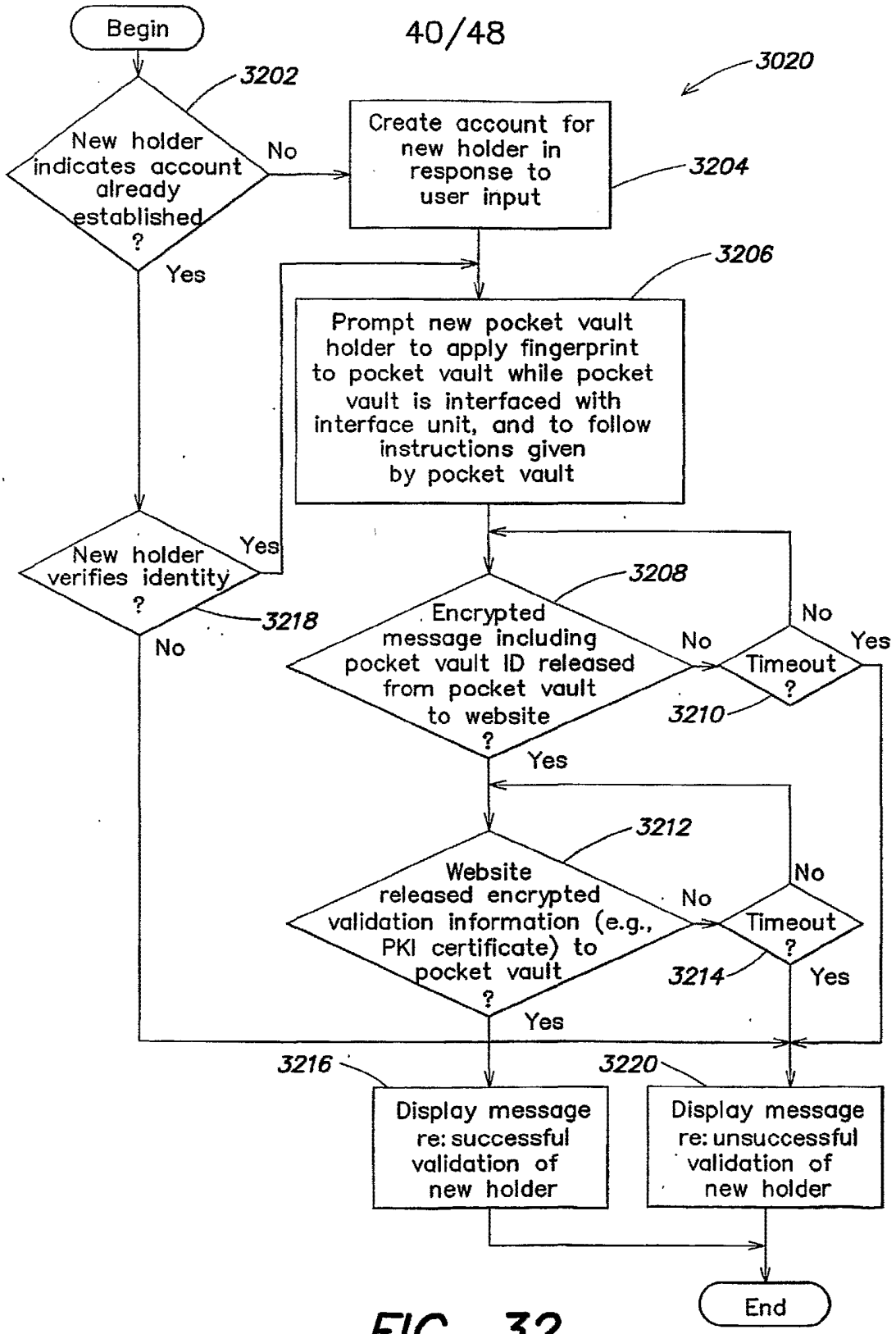

Begin
3202
New holder indicates account already established ?
No
Yes
3020
Create account for new holder in response to user input
3204
3206
Prompt new pocket vault holder to apply fingerprint to pocket vault while pocket vault is interfaced with interface unit, and to follow instructions given by pocket vault
New holder verifies identity ?
Yes
No
3218
3208
Encrypted message including pocket vault ID released from pocket vault to website ?
No
Yes
Timeout ?
No
Yes
3210
3212
Website released encrypted validation information (e.g., PKI certificate) to pocket vault ?
No
Yes
Timeout ?
No
Yes
3214
3216
3220
Display message re: successful validation of new holder
Display message re: unsuccessful validation of new holder
End

FIG. 32

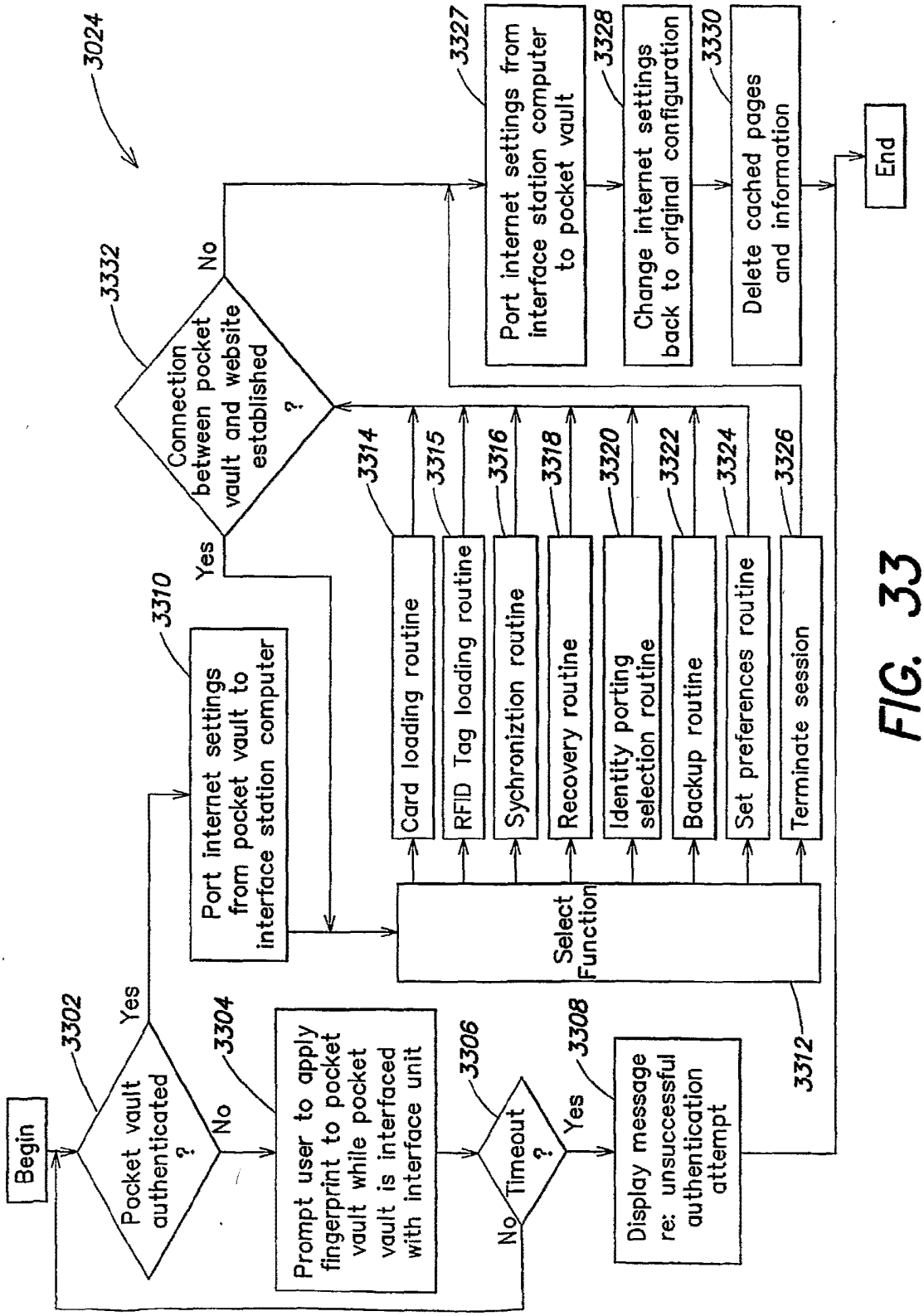

3024
Begin
3302
Pocket vault authenticated ?
Yes
No
3304
Prompt user to apply fingerprint to pocket vault while pocket vault is interfaced with interface unit
3306
Timeout ?
No
Yes
3308
Display message re: unsuccessful authentication attempt
3310
Port internet settings from pocket vault to interface station computer
3312
Select Function
3314
Card loading routine
3315
RFID Tag loading routine
3316
Sychroniztion routine
3318
Recovery routine
3320
Identity porting selection routine
3322
Backup routine
3324
Set preferences routine
3326
Terminate session
3327
Port internet settings from interface station computer to pocket vault
3328
Change internet settings back to original configuration
3330
Delete cached pages and information
End
3332
Connection between pocket vault and website established ?
Yes
No

FIG. 33

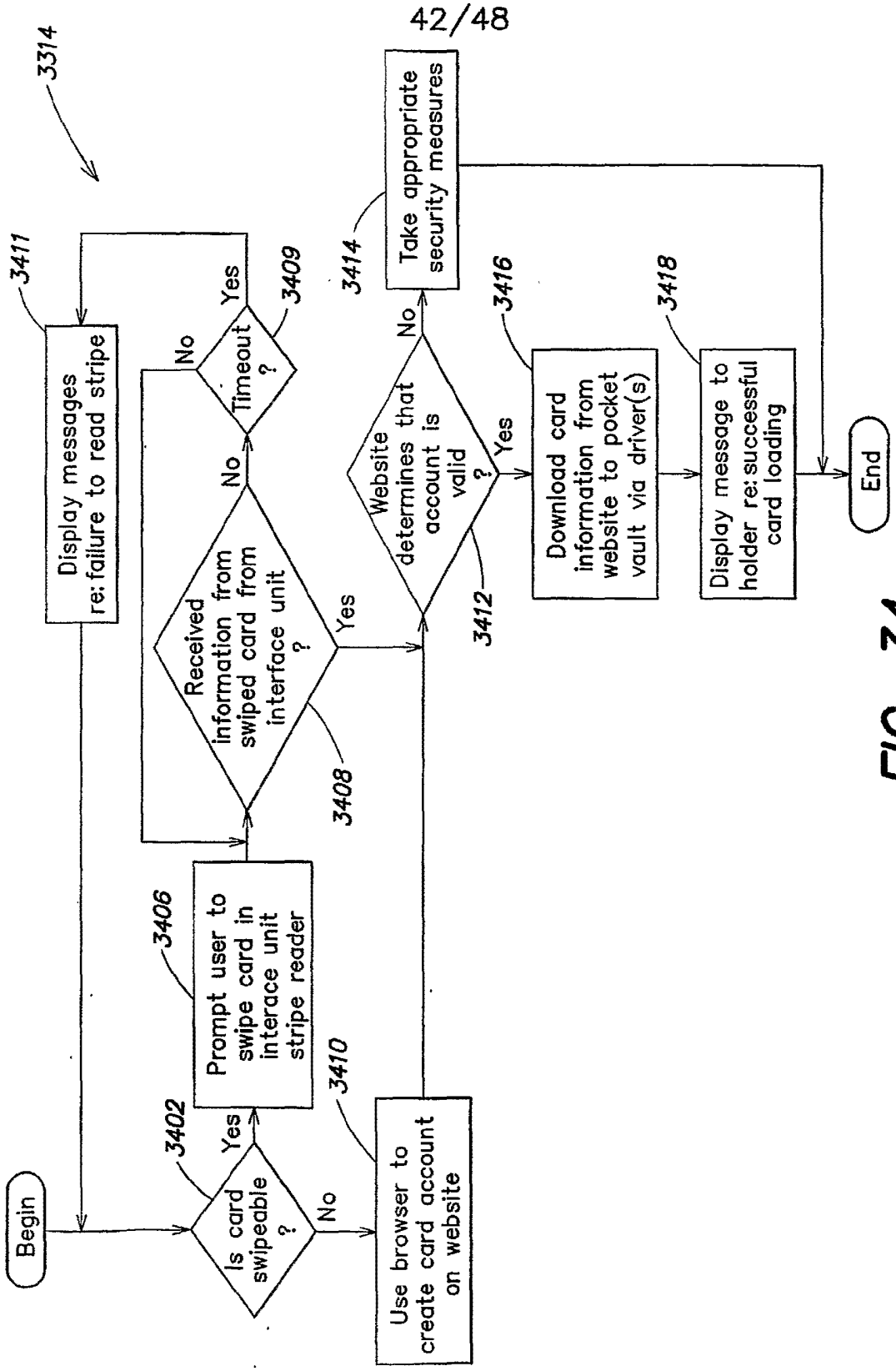

3314
Begin
Is card swipeable ?
3402
Yes
No
Prompt user to swipe card in interace unit stripe reader
3406
Use browser to create card account on website
3410
Received information from swiped card from interface unit ?
3408
Yes
No
Timeout ?
3409
Yes
No
Display messages re: failure to read stripe
3411
Website determines that account is valid ?
3412
Yes
No
Take appropriate security measures
3414
Download card information from website to pocket vault via driver(s)
3416
Display message to holder re: successful card loading
3418
End

FIG. 34

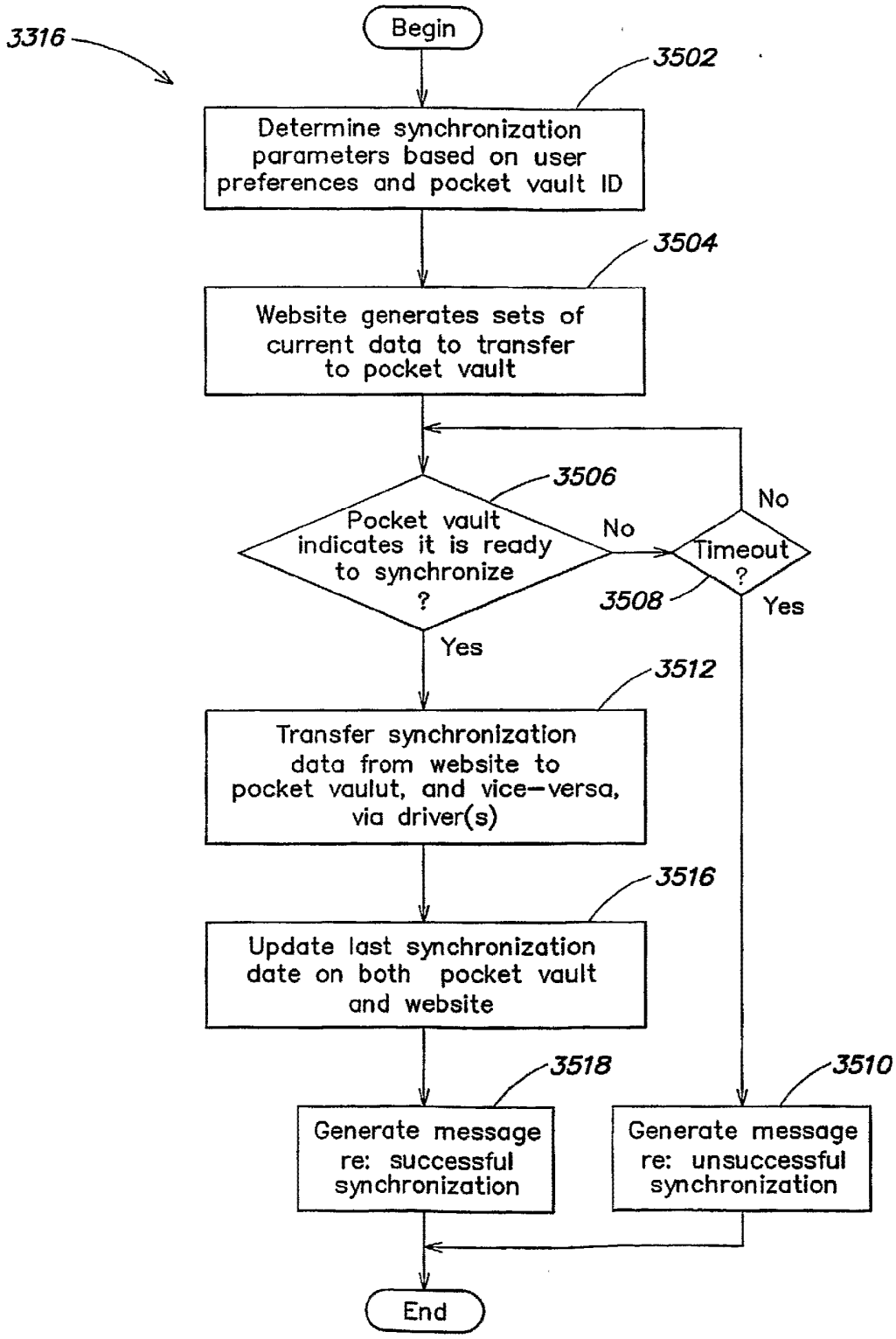

3316
Begin
3502
Determine synchronization parameters based on user preferences and pocket vault ID
3504
Website generates sets of current data to transfer to pocket vault
3506
Pocket vault indicates it is ready to synchronize ?
No
Timeout ?
3508
No
Yes
Yes
3512
Transfer synchronization data from website to pocket vaulut, and vice-versa, via driver(s)
3516
Update last synchronization date on both pocket vault and website
3518
Generate message re: successful synchronization
3510
Generate message re: unsuccessful synchronization
End

FIG. 35

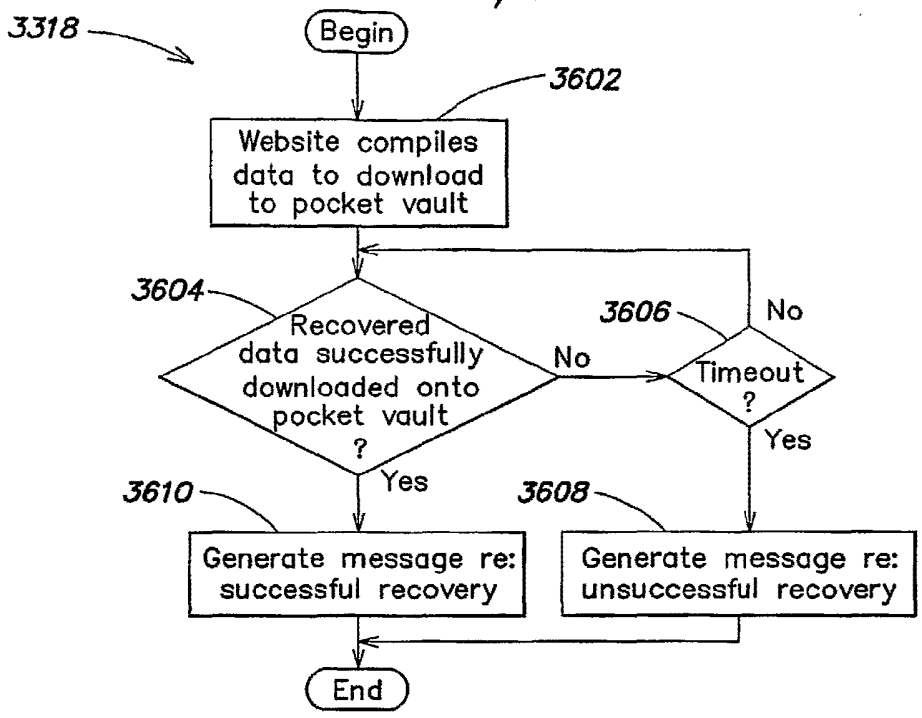

3318
Begin
3602
Website compiles data to download to pocket vault
3604
Recovered data successfully downloaded onto pocket vault ?
No
3606
Timeout ?
No
Yes
Yes
3610
Generate message re: successful recovery
3608
Generate message re: unsuccessful recovery
End

FIG. 36

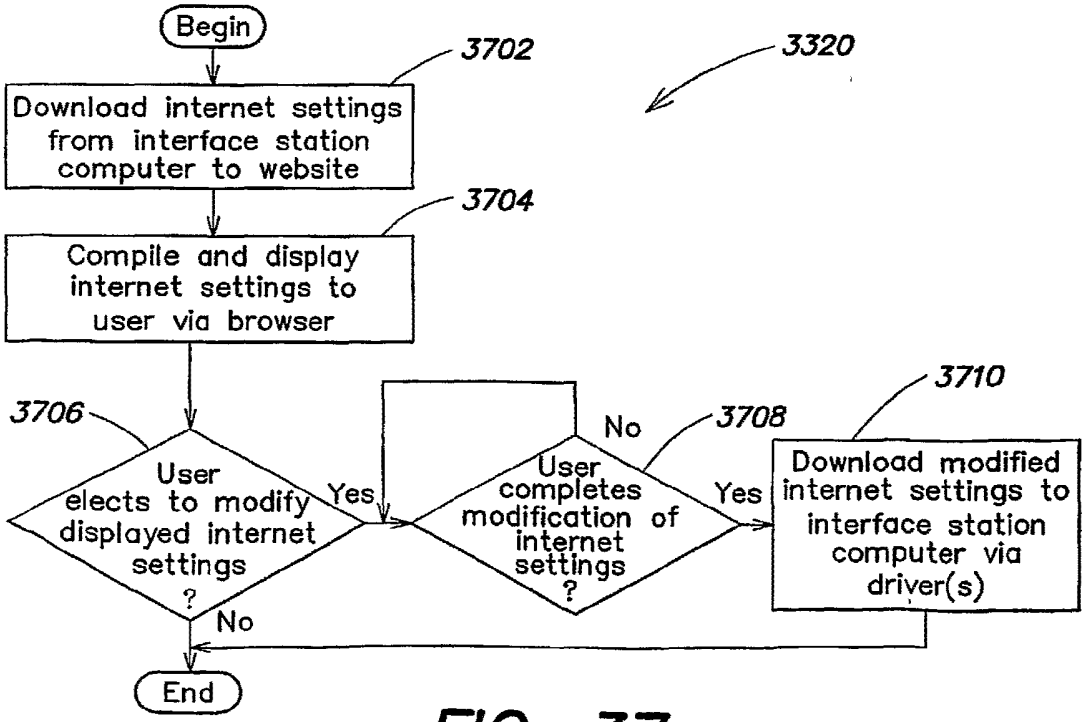

Begin
3702
Download internet settings from interface station computer to website
3320
3704
Compile and display internet settings to user via browser
3706
User elects to modify displayed internet settings ?
Yes
No
User completes modification of internet settings ?
No
3708
Yes
3710
Download modified internet settings to interface station computer via driver(s)
End

FIG. 37

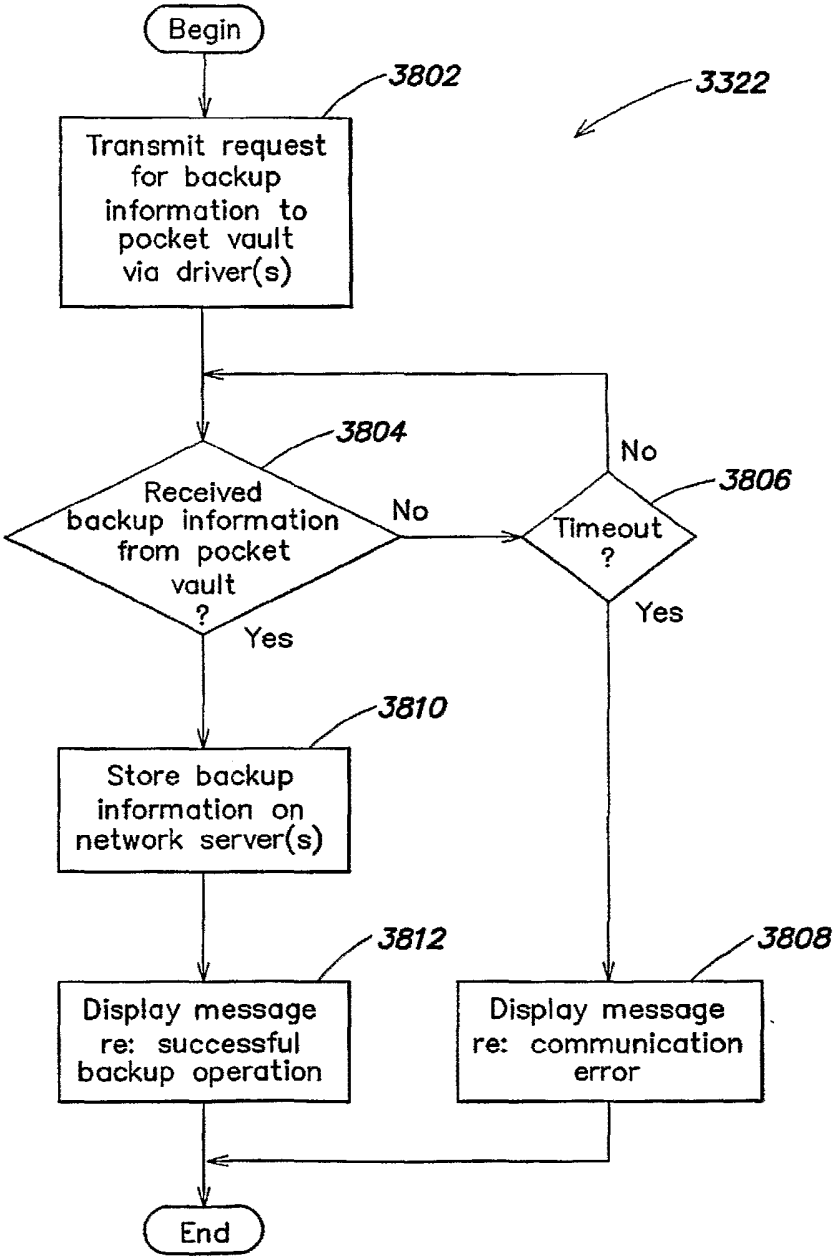

Begin
3802
3322
Transmit request for backup information to pocket vault via driver(s)
3804
Received backup information from pocket vault ?
No
Yes
3806
Timeout ?
No
Yes
3810
Store backup information on network server(s)
3812
Display message re: successful backup operation
3808
Display message re: communication error
End

FIG. 38

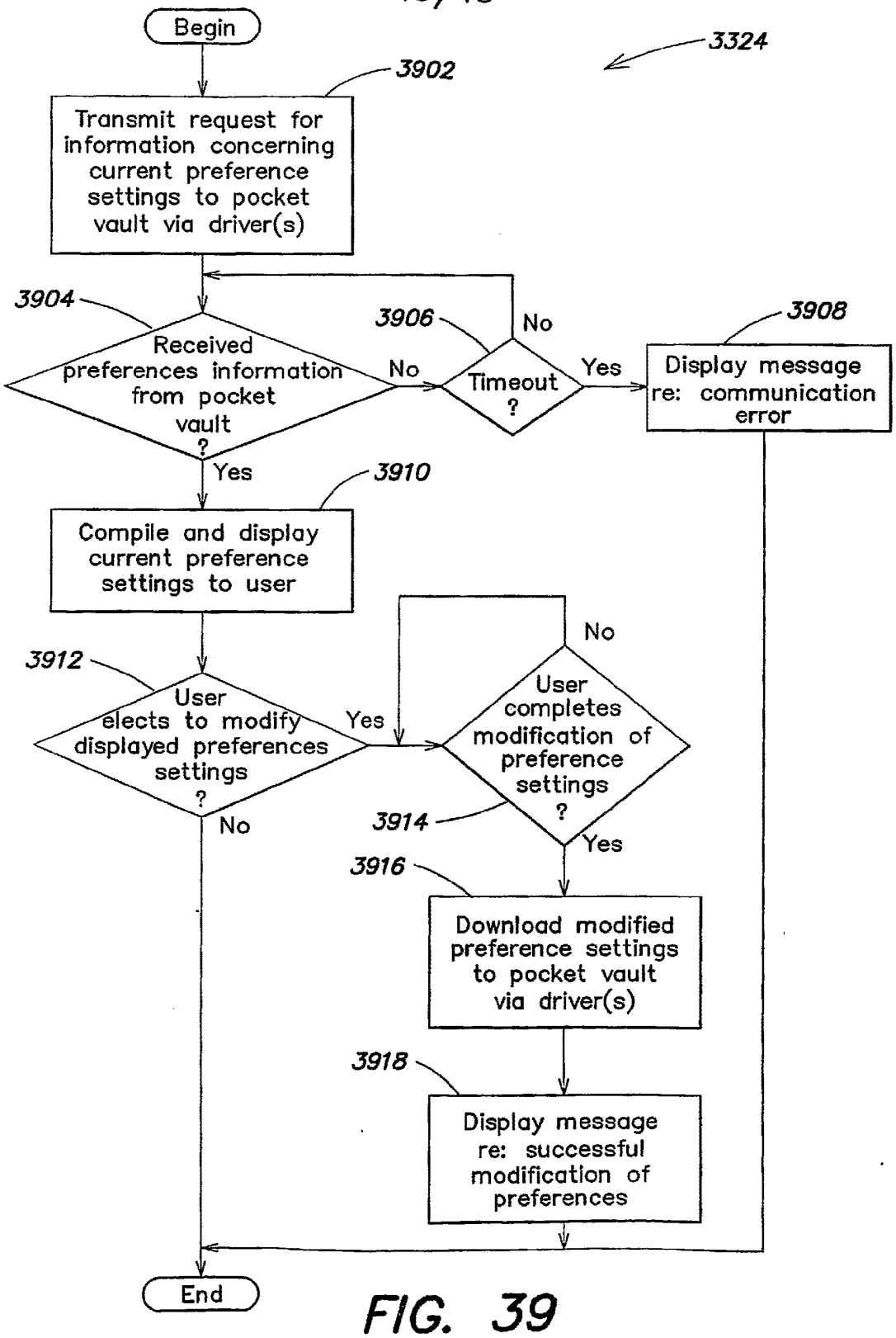

Begin
3324
3902
Transmit request for information concerning current preference settings to pocket vault via driver(s)
3904
Received preferences information from pocket vault ?
No
3906
Timeout ?
No
Yes
3908
Display message re: communication error
Yes
3910
Compile and display current preference settings to user
3912
User elects to modify displayed preferences settings ?
Yes
No
User completes modification of preference settings ?
No
3914
Yes
3916
Download modified preference settings to pocket vault via driver(s)
3918
Display message re: successful modification of preferences
End

FIG. 39

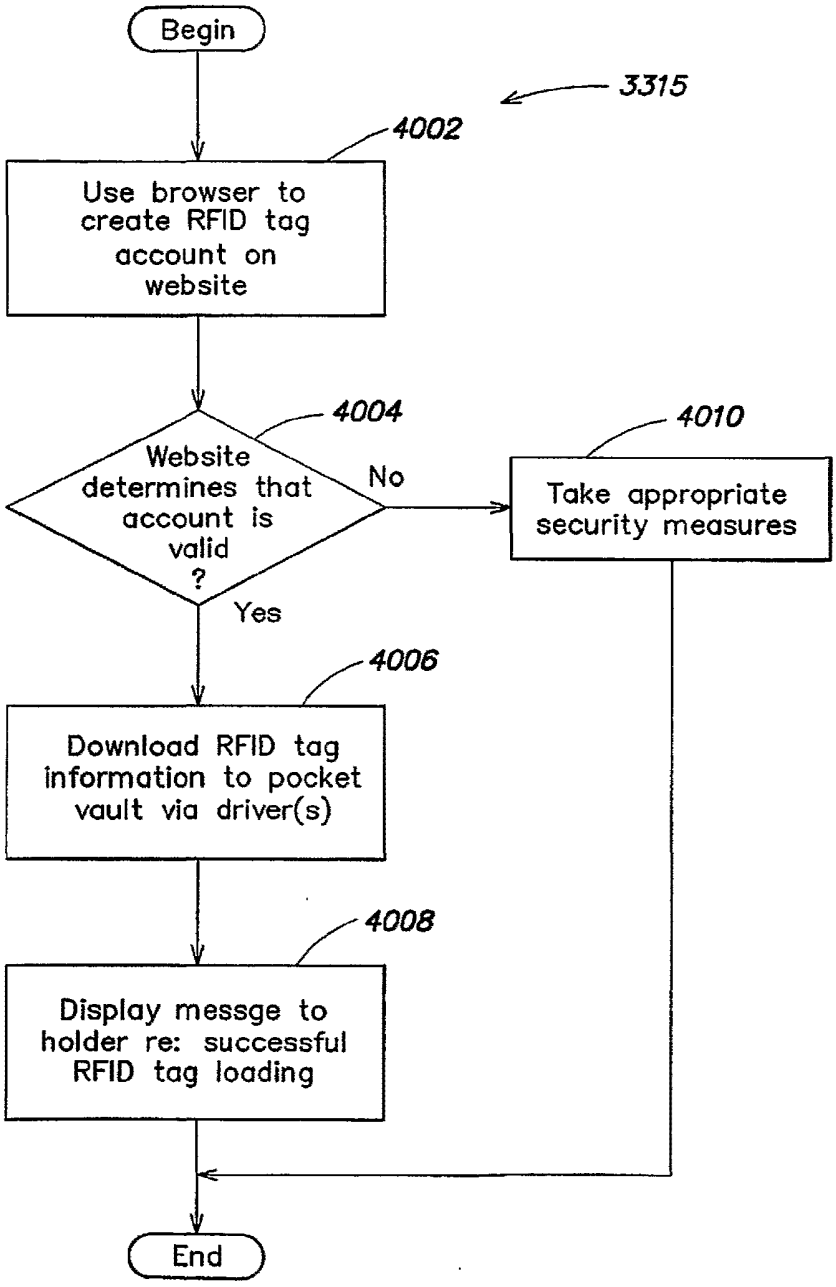

Begin
3315
4002
Use browser to create RFID tag account on website
4004
Website determines that account is valid ?
No
4010
Take appropriate security measures
Yes
4006
Download RFID tag information to pocket vault via driver(s)
4008
Display messge to holder re: successful RFID tag loading
End

FIG. 40

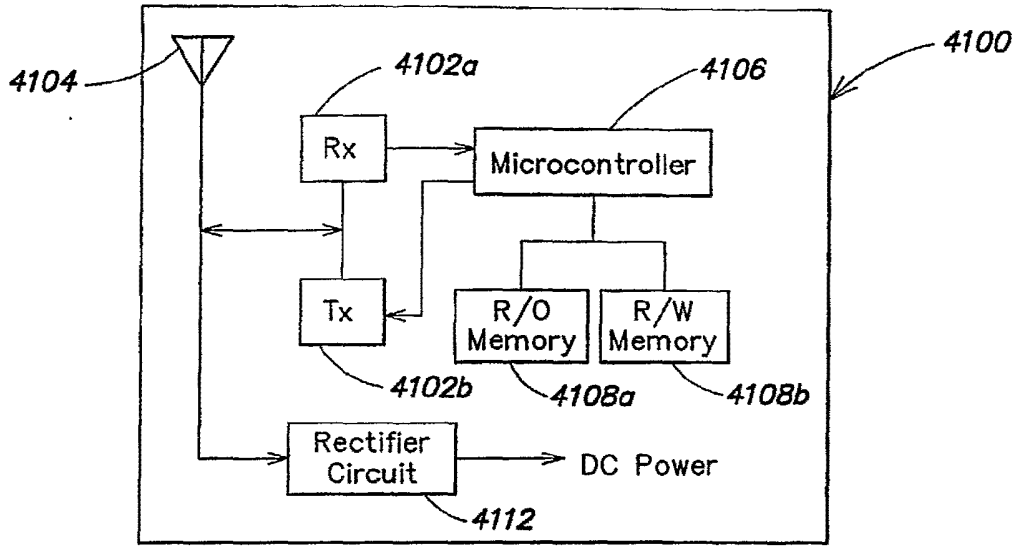


FIG. 41
(PRIOR ART)

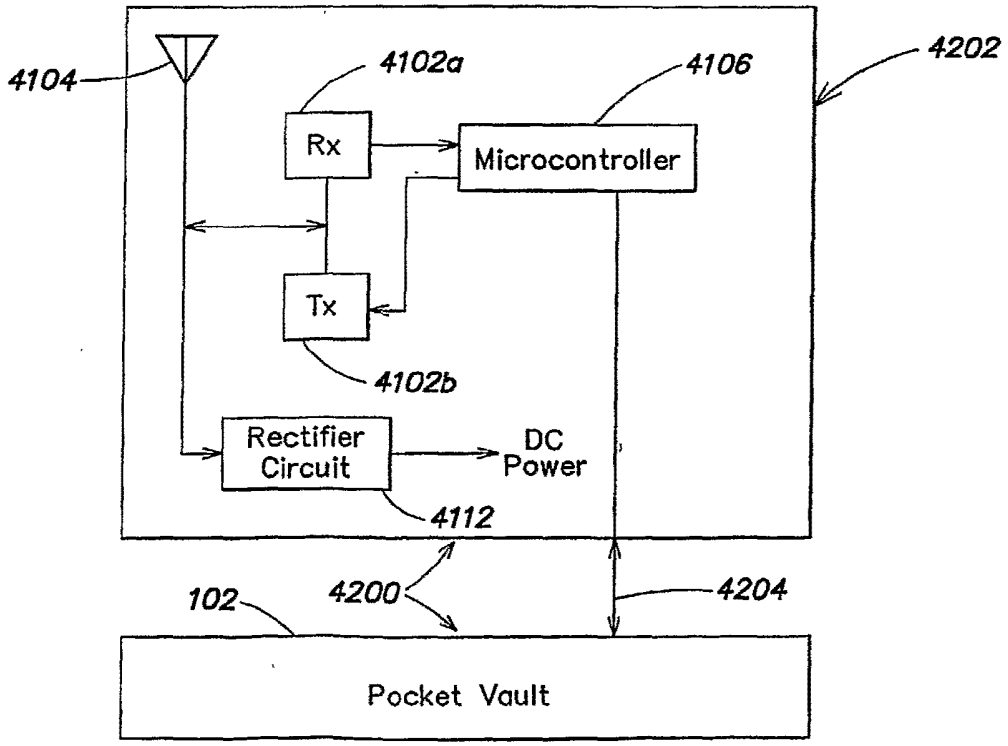


FIG. 42

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
5 February 2004 (05.02.2004)

PCT

(10) International Publication Number
WO 2004/012352 A1

(51) International Patent Classification[7]: H04B 1/38

(21) International Application Number: PCT/US2003/023080

(22) International Filing Date: 24 July 2003 (24.07.2003)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/399,686 30 July 2002 (30.07.2002) US

(71) Applicant *(for all designated States except US)*: **WAY SYSTEMS, INC.** [US/US]; 151 Mystic Avenue, Medford, MA 02155 (US).

(71) Applicants and
(72) Inventors: **GOLDTHWAITE, Scott** [US/US]; 15 Oregon Court, Hingham, MA 02043 (US). **GRAYLIN, William** [US/US]; 229 Washington Street, Woburn, MA 01801 (US).

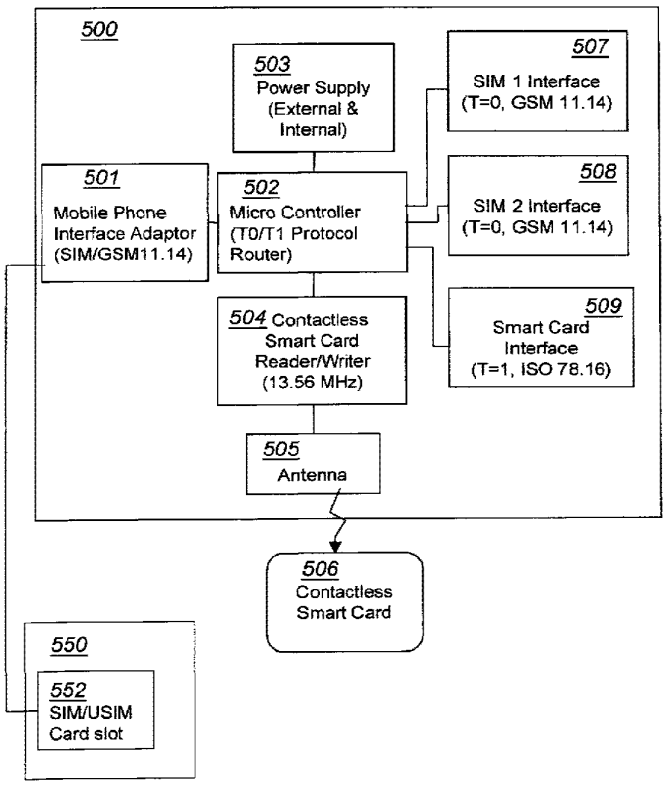
(74) Agent: **COLLINS, Aliki, K.**; AKC Patents, 215 Grove Street, Newton, MA 02466 (US).

(81) Designated States *(national)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NO, NZ, 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) 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, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, 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: MOBILE DEVICE EQUIPPED WITH A CONTACTLESS SMART CARD READER/WRITER



(57) Abstract: A wireless mobile device (550) is adapted to access a wireless network and includes a subscriber identification module (SIM) card slot (552) and a contactless smart card module (500) electrically connected to the SIM card slot (552) and thereby to the wireless mobile device (550). The contactless smart card module (500) is adapted to receive and read information stored in a contactless smart card (506) and transmit this information to an entity through the wireless mobile device (550) and the wireless network. The wireless mobile device (550) of this invention is used to conduct financial transactions using the contactless smart card (506). The financial transactions include face-to-face or remote purchases, payment with electronic cash stored in the contactless smart card, or payment with the contactless smart card through a financial institution, and downloading and storing of digital goods or services in the contactless smart card.

WO 2004/012352 A1

Declarations under Rule 4.17:

— *as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii)) for the following designations 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, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, 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, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG)*

— *as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii)) for the following designations 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, SC, SD, SE, SG, SK, SL, TJ, TM, TN, TR, TT, TZ, UA, UG, UZ, VC, VN, YU, ZA, ZM, ZW, 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, HU, IE, IT, LU, MC, NL, PT, RO, SE, SI, SK, TR), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, 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.

MOBILE DEVICE EQUIPPED WITH A CONTACTLESS SMART CARD READER/WRITER

Cross Reference to related Co-Pending Applications

This application claims the benefit of U.S. provisional application Serial No. 60/399,686 filed on July 30, 2002 and entitled MOBILE DEVICE EQUIPPED WITH A CONTACTLESS SMART CARD READER which is commonly assigned and the contents of which are expressly incorporated herein by reference.

Field of the Invention

The present invention relates to mobile devices, and more particularly to a mobile device that is equipped with a contactless smart card reader/writer for conducting financial transactions with a contactless smart card.

Background of the Invention

The use of contactless smart cards, as defined in prior art US Patent Number 4,480,178, has experienced rapid growth particularly in the use of transit systems such as MiFare™ (developed by Phillips Semiconductors) and Octopus Cards (developed by Sony). These types of smart cards create a secure environment for storing monetary value while the contactless feature is fast and convenient for users who only need to bring the card in close proximity to a card reader. These types of contactless cards do not require a Personal Identification Number (PIN) and are therefore suited for high-volume, low-value transactions. Users of the card can load value onto the card by using an Automated Teller Machine (ATM) or a kiosk to transfer money from a checking account, savings account, a credit card account or by inserting cash into the ATM. The user puts their ATM card or cash into the machine and positions a contactless card near the contactless reader/writer to complete the transfer of money. These ATMs are typically located at the entrance to the transit station where the customers purchase transit tokens. The popularity of contactless cards for transit has grown so that other vendors in area surrounding the transit system also accept the contactless card for payment for purchases such as parking, fast food, convenience stores and vending machines. Many merchants are installing contactless smart card reader/writers in their stores to provide the ability to accept contactless smart cards as

a form of payment. Because contactless smart card readers are required to load value onto a card and take value off of a card, the amount of readers in the marketplace is a key factor in determining the amount of usage of the contactless smart card.

The idea of adding a contactless reader/writer to a mobile phone is established in PCT WO 01/86599 A2, entitled "Smart Card Communications". However, this prior art application specifies that the connection between the contactless reader/writer and the mobile phone is through "an interface connector such as those used for connecting to a regular data modem". These type of interface connectors need to be customized for each type of mobile phone and the specific network that is connected to. Accordingly, there is a need for a universal connector that can be used in all types of mobile phones and all networks.

The general concept of a universal connector that can connect to any type of mobile phone and network is described in PCT patent application No. WO 99/66752, entitled "Communication Method and Apparatus Improvements", the entire content of which is incorporated herein by reference. Referring to FIG. 2, this universal connector 200 connects to the mobile phone's existing Subscriber Identification module (SIM) slot 204 and utilizes a Central Processor Unit (CPU) 202 to coordinate the activities of multiple SIM cards 152, 156 and a full-size external smart card 153. This universal connector may be implemented as an attachment to a mobile phone or may be embedded in the mobile phone. Although this implementation includes several SIM cards and a card reader for regular contact type smart cards, it does not include a contactless smart card reader/writer. Accordingly, there is still a need for a universal contactless smart card reader/writer that can be attached to any phone and any network.

Summary of the Invention

In general, in one aspect the invention features a wireless mobile device adapted to access a wireless network. The wireless mobile device includes a subscriber identification module (SIM) card slot and a contactless smart card module electrically connected to the SIM card slot and thereby to the wireless mobile phone. The contactless smart card module is adapted to receive and read information stored in a

contactless smart card and transmit this information to an entity via the wireless mobile device and the wireless network.

Implementations of this aspect of the invention may include one or more of the following features. The contactless smart card module is further adapted to receive information from the entity via the wireless network and transmit and write this information in the contactless smart card. The information may include cardholder identification information, card identification information, authentication information, smart card issuer information, financial institution information, digital goods, digital services, or digital currency. The digital goods include electronic cash, electronic coupons, electronic gift certificates, electronic transit tokens, music, software, movies, and books. The wireless mobile device may further include a memory; a SIM card connected to the SIM card slot and authenticating the wireless mobile device to the wireless network, a Central Processing Unit (CPU) and a first application program associated with the memory and the CPU and being adapted to receive and transmit instructions from the contactless smart card module to the wireless mobile phone and the reverse. The wireless mobile device may further include a second application program associated with the memory and the CPU and being adapted to route and transmit data and information among the wireless mobile phone, the smart card module, and other interfaces connected to the CPU. These other interfaces may be smart card interfaces, infrared transceiver interfaces, serial communication interfaces, or magnetic stripe reader interfaces. The first and second application programs may be stored in the CPU, the SIM card, an external SIM card, the contactless smart card, or an external card. The wireless mobile device may also include an antenna for receiving and transmitting messages to and from the contactless smart card. The wireless mobile device may be a mobile phone, a personal digital assistant, a pager, a wireless laptop computer, a personal computer, a television remote control, and combinations thereof. The wireless network may be a wireless wide area network (WWAN), a wireless local area network (WLAN), a private network, or a personal area network (PAN). The wireless wide area network (WWAN) may be a Global System for Mobile Communications (GSM), a Code Division Multiple Access (CDMA), CDMA 2000, or wideband CDMA (WCDMA). The wireless mobile device may be used for making financial transactions between a user and an entity

IPR2025-00644 Page 00956

with the contactless smart card over the network. The financial transactions between the user and the entity may be face-to-face or remote.

In general, in another aspect the invention features an electronic communication method including purchasing a good or a service from a merchant, and paying with a contactless smart card via a wireless mobile device. The wireless mobile device is adapted to access a wireless network and includes a subscriber identification module (SIM) card slot and a contactless smart card module electrically connected to the SIM card slot and thereby to the wireless mobile device. The contactless smart card module is adapted to receive and read information stored in the contactless smart card and transmit the information to an entity via wireless mobile device and the wireless network.

Implementations of this aspect of the invention may include one or more of the following features. The electronic communication method may further include receiving the good or service electronically, storing it in the contactless card, retrieving the good or service from the contactless card and redeeming it.

In general, in another aspect the invention features an electronic payment method utilized by a customer to pay a merchant with electronic cash stored in a contactless smart card for a face-to-face purchase of a good or service. The method includes placing an order by the customer for the purchase of the good or service to the merchant and providing a wireless mobile device wherein the mobile device is adapted to access a wireless network and comprises a subscriber identification module (SIM) card slot and a contactless smart card module electrically connected to the SIM card slot and wherein the contactless smart card module is adapted to receive and read information stored in the contactless smart card and transmit the information via the wireless network. Next, entering information of the purchase in the wireless mobile phone, positioning the contactless smart card in close proximity to the wireless mobile device and retrieving smart card identification information and authorizing withdrawal of an electronic cash amount for payment for the good or service from the smart card. Next, sending the purchase information, the smart card identification information and the electronic cash amount to an authentication server via the wireless network, and authenticating and sending the purchase information and the

IPR2025-00644 Page 00957

electronic cash amount by the authentication server to a business account of the merchant held in a financial institution. Next, registering the purchase information and depositing the electronic cash amount to the merchant's business account and sending confirmation by the financial institution to the authentication server. Finally, forwarding the confirmation to the wireless mobile phone and fulfilling the order to the customer by the merchant.

In general, in yet another aspect the invention features an electronic payment method utilized by a customer to pay a merchant with a contactless smart card for a face-to-face purchase of a good or service. The method includes placing an order by the customer for the purchase of the good or service to the merchant and providing a wireless mobile device wherein the wireless mobile device is adapted to access a wireless network and comprises a subscriber identification module (SIM) card slot and a contactless smart card module electrically connected to the SIM card slot and wherein the contactless smart card module is adapted to receive and read information stored in the contactless smart card and transmit the information via the wireless network. Next, entering information of the purchase in the wireless mobile phone, positioning the contactless smart card in close proximity to the wireless mobile device, and retrieving smart card identification information from the contactless smart card and authorizing payment for the good or service. Next, formatting the purchase information, the smart card identification information and the payment authorization into a first message and sending the first message to an authentication server via the wireless network, and authenticating and sending the first message by the authentication server to a financial institution. Next, registering the purchase information and sending approval for the payment by the financial institution to the authentication server. Finally, forwarding the payment approval to the wireless mobile phone and fulfilling the order to the customer by the merchant.

In general, in yet another aspect the invention features an electronic payment method utilized by a customer to pay a merchant with a contactless smart card for a remote purchase of a good or service. The method includes placing an order by the customer for the purchase of the good or service to a merchant server via a first network and choosing to pay via a wireless mobile device wherein the wireless mobile device is adapted to access a wireless network and comprises a subscriber identification module

IPR2025-00644 Page 00958

(SIM) card slot and a contactless smart card module electrically connected to the SIM card slot and wherein the contactless smart card module is adapted to receive and read information stored in the contactless smart card and transmit the information via the wireless network. Next, providing the merchant server with an identification information for the wireless mobile device and creating a digital order comprising purchase information and the identification number for the wireless mobile device by the merchant server. Next, routing the digital order to an authentication server via the first network, formatting the digital order into a first message wherein the first message is adapted to be transmitted over the wireless network and routing the first message over the wireless network to the wireless mobile device. Next, displaying the first message on the wireless mobile device, and requesting and receiving authorization of payment from the customer via the wireless mobile device. Next, positioning the contactless smart card in close proximity to the wireless mobile device, retrieving smart card identification and security information, and formatting authorization result and smart card identification and security information into a second message and routing the second message to the authentication server. Next, authenticating and routing the second message to a financial institution, wherein the financial institution is the issuer of the contactless smart card. Finally, approving and executing the payment at the financial institution, forwarding the payment approval to the authentication server and from the authentication server to the wireless mobile phone and fulfilling the order to the customer by the merchant.

Implementations of this aspect of the invention may include one or more of the following features. The good or service may be a digital good or a digital service and the fulfilling includes downloading and storing the digital good or service in the contactless smart card. The digital good may be electronic cash, electronic coupons, electronic gift certificates, electronic transit tokens, music, software, movies, or books. The wireless mobile device may be a mobile phone, a personal digital assistant, a pager, a wireless laptop computer, a personal computer, a television remote control, or combinations thereof. The wireless network may be a wireless wide area network (WWAN), a wireless local area network (WLAN), a private network, or a personal area network (PAN). The wireless wide area network (WWAN) may be a Global System for Mobile Communications (GSM), a Code Division Multiple Access (CDMA), CDMA 2000, or wideband CDMA (WCDMA).

The first and second messages may be formatted in Short Message Service (SMS), General Packet Radio Service (GPRS), Transmission Control Protocol/Internet Protocol (TCP/IP), User Datagram Protocol (UDP), Simple Mail Transmission Protocol (SMTP), Simple Network Management Protocol (SNMP), or proprietary message formats.

Among the advantages of this invention may be one or more of the following. Combining a contactless smart card reader with a wireless mobile device can dramatically increase the number of smart card reader points of sales (POS) in the marketplace. The increased number of POS offers convenience to consumers and more opportunities to merchants. Consumers with wireless mobile devices equipped with a smart card reader can load value to their contactless cards anytime and anywhere and may use their contactless smart cards for mobile commerce purchases with the mobile device such as ring tones, mobile airtime credits and other types of remote purchases. Merchants that do not have the ability to install a traditional contactless smart card reader/writer that requires power from an electrical outlet and integration with a cash register would also benefit from a mobile contactless reader/writer for many types of transactions. These merchants include taxi cabs, vending machines and "push cart" vendors. Additionally, a wireless mobile device equipped with a contactless smart card reader enables "peer-to-peer" transfer of money using contactless cards.

The invention defined in this application specifies that the contactless smart card module connects to the wireless mobile device through the Subscriber Identification Module (SIM) circuitry on a GSM mobile phone. This configuration allows the contactless smart card module to function as any other type of smart card module as specified in the GSM 11.14 communication standards and enables any GSM phone that supports GSM 11.14 to utilize the contactless smart card module. The advantage to this standards-based design enables any application to access the contactless smart card module using GSM 11.14 commands (i.e. Power On Card, Read Card) without having to make modifications to the mobile device itself. Although a mobile device may have many external interface points (i.e. serial, USB, Bluetooth, Infrared), these communication protocols, while standard, are implemented differently for each mobile device, therefore connecting a contactless smart card reader to any other

IPR2025-00644 Page 00960

interface point on the mobile device would require a specific interface application developed for each mobile device. Most mobile devices do not allow applications to be installed or modified on the device once the device has been distributed to customers. The advantage of the present invention is that the contactless smart card module can be used to retrofit any mobile device that does not allow reprogramming with or without the permission or knowledge of the mobile device manufacturer or the mobile network operator.

Another advantage of the present invention is the creation of many types of systems and methods for using contactless smart cards for purchasing and fulfillment of goods and services because of the network connectivity established by the connected mobile device. As was mentioned above, the present invention provides a POS system for mobile merchants (i.e. taxi cab drivers and fast food vendors) and allows them to accept contactless smart cards as a form of payment. The present invention also enables consumers to make remote purchases using contactless smart cards as a method of payment. Finally, the present invention provides consumers with the ability to purchase and download digital goods such as coupons, transit coupons and electronic cash (e-Cash) to a contactless smart card.

Brief Description of the Drawings

FIG. 1 illustrates a circuitry according to this invention for a contactless smart card reader/writer module that converts a Single-SIM GSM phone into a Dual-SIM/Dual-Slot GSM phone with a contactless smart card reader/writer;

FIG. 2 illustrates a prior art circuitry for a mobile device attachment that converts a Single-SIM GSM phone into a Dual-SIM/Dual-Slot GSM phone with an external card reader;

FIG. 3 illustrates a mobile phone with the contactless smart card reader/writer module of FIG. 1 and a contactless smart card ;

FIG. 4 is a schematic diagram of a payment system utilizing the mobile phone of FIG. 3 for a face-to-face purchase according to this invention;

IPR2025-00644 Page 00961

FIG. 5 is a schematic diagram of a payment system utilizing the mobile phone of FIG. 3 for remote purchases according to this invention;

FIG. 6 is a flow diagram of the remote payment system of FIG. 4;

FIG. 7 is a schematic diagram of a payment system for digital goods purchase and fulfillment using the mobile device of FIG. 3; and

FIG. 8 is a flow diagram of the payment and digital goods fulfillment system of FIG. 7.

Detailed Description of the Invention

Referring to FIG. 1, a contactless smart card reader/writer module 500 is connected to a wireless mobile phone 550 through a Subscriber Identification Module/Universal Subscriber Identification Module (SIM/USIM) card slot 552. The contactless smart card reader/writer module 500 includes a mobile phone interface adaptor (501) that connects to the Subscriber Identification Module/Universal Subscriber Identification Module (SIM/USIM) card slot circuitry 552 of the wireless mobile phone 550. In one example, the mobile phone interface adaptor 501 is described in WO 99/66752 application and US 6,292,561 patent. The entire content of WO 99/66752 application and US 6,292,561 patent is incorporated herein by reference. The contactless smart card reader/writer module 500 further includes a Micro Controller or Central Processing Unit (CPU) 502 that controls the mobile phone interface adaptor 501 and manages the routing of communications and controls between the mobile phone 550 and the contactless smart card reader/writer 504 as well as a plurality of smart cards. In addition to the contactless smart card reader/writer 504, module 500 includes a memory (not shown), SIM card interfaces 507, 508, adapted to receive SIM cards, and a smart card interface 509 that accepts regular contact-type smart cards. The CPU 502 receives commands from the mobile phone 550, analyzes the commands and routes those commands to the appropriate interface. The contactless smart card reader/writer 504 is connected to an antenna 505 that is mounted externally to the module or is embedded into the module's Printed Circuit Board (PCB). In other embodiments the antenna 505 is connected directly to the mobile phone 550. The contactless smart card reader/writer 504 receives activation commands and

IPR2025-00644 Page 00962

instructions via the CPU 502 from an application on any of the interfaces connected to the CPU 502, including an application on the mobile device interface 501, an application on the mobile phone 550, an application on the SIM Interface 507, an application on the SIM Interface 508, an application on the smart card Interface 509 or an application on the CPU itself. Using the antenna 505, module 500 receives and transmits information to and from a contactless smart card 506 using standard communication protocols as specified by ISO 14443 A/B and ISO 15693 standards using 13.56 MHz and 125 kHz frequencies. Module 500 is powered by a power supply 503 which may be either internal to the module or external.

Referring to FIG. 3, for existing mobile phones, the module 500 is an attachment that connects to the existing SIM slot on the mobile phone 550. The module 500 may also be embedded within the mobile device. In either case, the mobile phone 550 receives and transmits information to and from a contactless smart card 506 when the contactless card 506 is brought in close proximity to the mobile phone 550.

One embodiment of the present invention provides a contactless smart card payment system where the user of the mobile phone equipped with a contactless smart card reader is able to accept contactless smart cards as a form of payment for face-to-face purchases. Referring to FIG. 4, a payment transaction system 100 for a face-to-face purchase of a product or a service includes a customer 102 with a contactless smart card, a merchant with a mobile device 110 equipped with a contactless smart card reader, a payment server 106, an authentication server 107, and a financial institution 112. The authentication server 107 receives and transmits messages in a short message service (SMS) format to the merchant's mobile phone 110 via an SMS carrier through a wireless Global System for Mobile Communication (GSM) network 90. The mobile phone 110 receives and transmits information from and to a contactless smart card. After completing the purchase of a product or a service with the merchant, the customer 102 provides the merchant with the contactless smart card to pay for the purchase. The merchant activates a mobile payment application on the mobile device 110 and positions the contactless smart card in close proximity to the mobile device. The contactless smart card reader activates the application on the contactless smart card using wireless smart cards communication protocol 70. Using the contactless reader on the mobile phone 110, the payment application on the

IPR2025-00644 Page 00963

mobile device sends the appropriate commands to the smart card to deduct from the smart card the amount for the purchase. The mobile phone 110 encrypts the transaction information and sends a message to the authentication server 107 over the wireless GSM network 90. The message includes the merchant vendor information, type of purchase and the amount due. The authentication server 107 validates the transaction information from the mobile device, decrypts the transaction information and routes the transaction information to the payment server 106 over communication network 80. The payment server 106 connects to the merchant's financial institution 112 over communication network 80. The financial institution 112 processes the payment, updates the merchant's account and sends a confirmation of the payment to the payment server 106. The payment server 106 routes the payment confirmation to the authentication server 107. The authentication server 107 encrypts and sends a message confirming the payment to the merchant's mobile device 110. In one example, the authentication server 107 is described in a co-pending patent application entitled " System and method for payment transaction authentication", the entire content of which is incorporated herein by reference.

In another embodiment, the present invention provides a contactless smart card payment system for consumers making remote purchasing and payment transactions. Referring to FIG. 5 and FIG. 6, a payment transaction system 300 includes a customer 102, a merchant server 104, a payment server 106, an authentication system 108, and a financial institution 112. The authentication system 108 includes an authentication server 107 that is adapted to send and receive messages in a short message service (SMS) format to a mobile phone 110 via an SMS carrier 109. The mobile phone 110 is adapted to receive a contactless smart card (not shown). After having placed an order for an item or a service through a personal computer (PC) connected via the Internet 80 to the merchant server 104, a customer 102 is asked to choose a payment method. The customer 102 chooses to pay via her mobile phone 110 and gives her mobile phone identification information to the merchant server 104 (114). In one example, the mobile phone identification information is the mobile phone number. The merchant server 104 routes the customer's mobile phone number and information about the purchase order to a payment server 106 (116). The payment server 106 contacts the authentication server 107 and routes the customer's mobile phone number and information about the purchase (118). The authentication server 107

sends an SMS message to the customer's mobile phone 110 through an SMS carrier 109 (120). The customer 102 receives the SMS message asking her to authorize the purchase and choose a payment card (122). The customer 102 authorizes the purchase, positions the contactless smart card in proximity to her mobile phone 110, and enters a security code (if required) to pay and authenticate her purchase (124). In one example, the security code is a personal identification number (PIN). Other examples include a password, digital signature, and a biometric identifier, i.e., retina scan, fingerprint, DNA scan, voice characteristics. The payment card is identified with information that is embedded in the card. In one example the identification information is a payment card number. Other examples of payment card identification include an encrypted transaction signature that can only be decrypted by the financial institution that has issued the payment card, expiration date of the payment card, and a digital signature. In another example the payment card may contain an electronic purse (e-Purse) with stored value (i.e. e-Cash, e-Coupon, e-Ticket) contained within the smart card and the amount of the transaction is deducted from the e-Purse. The mobile phone 110 sends an SMS message via the SMS Carrier 109 to the authentication server 107. The SMS message includes the authorization result (if required) and payment transaction information. The authentication server 107 routes the authorized purchase order and authenticated card information to the payment server 106 (128). If the transaction is not a stored value smart card transaction, the payment server 106 contacts the financial institution 112 that has issued the payment card and routes the payment card information and the purchase order information (130). If the transaction is a stored value transaction, the payment server 106 contacts the financial institution of the merchant and routes the payment transaction information. The financial institution 112 processes the payment transaction and sends a confirmation of the payment transaction to the payment server 106 (132). The payment server 106 routes the payment confirmation to the merchant server 104 (134) and to authentication server 107 (136). The authentication server 107 sends an SMS message confirming the payment transaction to the customer's mobile phone 110 (138). Finally the merchant 104 fulfills the customer's purchase order (140).

In another embodiment, the present invention provides a contactless smart card payment and digital goods fulfillment system. The contactless smart card has the

IPR2025-00644 Page 00965

ability to retain stored value or other types of information within the card. These "digital goods" are electronic, virtual information that represent value such as electronic cash (e-Cash), electronic coupons (e-Coupon), electronic tickets (e-Ticket), electronic transit tokens and digital media such as music, software, movies, books and other digital content. The payment transaction and digital goods fulfillment system allows the purchase of digital goods and reception and storage of the digital goods on the contactless smart card. Referring to FIG. 7 and FIG 6, a payment transaction and digital goods fulfillment system 600 includes a customer 102 with a contactless smart card and a mobile device 110 equipped with contactless smart card reader/writer 110, a merchant server 104, a payment server 106, an authentication system 108, a financial institution 112 and a fulfillment server 601. The authentication system 108 includes an authentication server 107 that is adapted to send and receive messages in a short message service (SMS) format to a mobile phone 110 via an SMS carrier 109. The mobile phone 110 is adapted to receive the contactless smart payment card . After having placed an order for digital goods via the Internet, SMS, WAP or voice 80, a customer 102 is asked to choose a payment method. The customer 102 chooses to pay via her mobile phone 110 and gives her mobile phone identification information to the merchant server 104 (114). In one example, the mobile phone identification information is the mobile phone number. The merchant server 104 routes the customer's mobile phone number and information about the purchase order to a payment server 106 (116). The payment server 106 contacts the authentication server 107 and routes the customer's mobile phone number and information about the purchase (118). The authentication server 107 sends an SMS message to the customer's mobile phone 110 through an SMS carrier 109 (120). The customer 102 receives the SMS message asking her to authorize the purchase and choose a payment card (122). The customer 102 authorizes the purchase, uses a smart card that is associated with her mobile phone 110, and enters a security code to pay and authenticate her purchase (124). In one example, the security code is a personal identification number (PIN). Other examples include a password, digital signature, and a biometric identifier, i.e., retina scan, fingerprint, DNA scan, voice characteristics. The payment card is identified with information that is embedded in the card. In one example the identification information is a payment card number. Other examples of payment card identification include an encrypted transaction signature that can only be decrypted by the financial institution that has issued the

IPR2025-00644 Page 00966

payment card, expiration date of the payment card, and a digital signature. The mobile phone 110 sends an SMS message via the SMS Carrier 109 to the authentication server 107. The SMS message includes the authorization result and payment transaction information (126). The authentication server 107 routes the authorized purchase order and authenticated card to the payment server 106 (128). The payment server 106 contacts the financial institution 112 that has issued the payment card and routes the payment card information and the purchase order information (130). The financial institution 112 processes the payment transaction and sends a confirmation of the payment transaction to the payment server 106 (132). The payment server 106 routes the payment confirmation to the merchant server 104 (134), presents a digital receipt to the fulfillment server 601 (602) and routes the payment confirmation to the authentication server 107 (136). The authentication server 107 sends an SMS message confirming the payment transaction to the customer's mobile phone 110 (138). Finally the fulfillment server 601 fulfills the customer's order for digital goods (140) by sending the electronic information that represents the digital goods to the authentication server 107. The authentication server 107 sends an SMS message to the customer's mobile phone 110 through an SMS carrier 109 (120). The mobile phone 110 receives the digital goods from the authentication server 107 and the customer 102 receives a message that digital goods are available for the contactless smart card. The customer 102 positions the contactless smart card in close proximity to the mobile phone 110 that is equipped with a contactless smart card reader/writer. The mobile phone 110 establishes a communication link 70 with the contactless smart card and transfers the digital goods to the contactless smart card.

Other embodiments are within the scope of the following claims. For example, the mobile phone identification information may be an Internet Protocol (IP) address. The communication networks 80, 82, 84, 86, 88 and 90 may be wireless or wired networks. The communication networks 80, 82, 84, 86, 88 and 90 may be non face-to-face via the Internet, VPN (Virtual Private Network), cable network, data network, telephone network, private voice and data networks, public voice and data networks, and mail or person to person. Payment card identification may occur via the payment card number or via an encrypted transaction signature that can only be decrypted by the financial institution that has issued the payment card. The authentication server may also utilize a password, digital signature, or a biometric identifier, i.e., retina

scan, fingerprint, voice characteristics, to authenticate the payment transaction. The payment authentication instrument may be contained in the contactless smart card, on the SIM smart cards within the mobile phone 110, or within another full-size smart card that needs to be inserted into a smart card reader slot. The communication between the authentication server 107 and the mobile phone 110 may be via a proprietary message protocol that utilizes User Datagram Protocol (UDP) on top of Internet Protocol (IP). This proprietary message protocol is adapted to be used with wireless networks that support Transmission Control Protocol/Internet Protocol (TCP/IP). These wireless networks include Bluetooth, 3G, GPRS, 2.5G, Infrared, 802.11a and 802.11b.

Several embodiments of the present invention have been described. Nevertheless, it will be understood that various modifications may be made without departing from the spirit and scope of the invention. Accordingly, other embodiments are within the scope of the following claims.

What is claimed is:

IPR2025-00644 Page 00968

1. A wireless mobile device adapted to access a wireless network comprising:

a subscriber identification module (SIM) card slot; and

a contactless smart card module electrically connected to said SIM card slot; and

wherein said contactless smart card module is adapted to receive and read information stored in a contactless smart card and transmit said information to an entity via said wireless network.

2. The wireless mobile device of claim 1 wherein said contactless smart card module is further adapted to receive information from said entity via said network and transmit and write said information in said contactless smart card .

3. The wireless mobile device of claim 1 wherein said information is selected from a group consisting of cardholder identification information, card identification information, authentication information, smart card issuer information, financial institution information, digital goods, digital services, and digital currency.

4. The wireless mobile device of claim 3 wherein said digital goods are selected from a group consisting of electronic cash, electronic coupons, electronic gift certificates, electronic transit tokens,, music, software, movies, and books.

5. The wireless mobile device of claim 1 further comprising;

a memory;

a Central Processing Unit (CPU);

a SIM card connected to said SIM card slot, said SIM card authenticating said wireless mobile device to said wireless network; and

a first application program associated with said memory and said CPU and being adapted to receive and transmit instructions from said contactless smart card module to said wireless mobile phone and the reverse.

IPR2025-00644 Page 00969

6. The wireless mobile device of claim 5 further comprising a second application program associated with said memory and said CPU and being adapted to route and transmit data and information among said wireless mobile phone, said smart card module, and other interfaces connected to said CPU.

7. The wireless mobile device of claim 6 wherein said other interfaces are selected from a group consisting of smart card interfaces, infrared transceiver interfaces, serial communication interfaces, and magnetic stripe reader interfaces.

8. The wireless mobile device of claim 6 wherein said first and second application programs are stored in storage selected from a group consisting of said CPU, said SIM card, an external SIM card, said contactless smart card , and an external card.

9. The wireless mobile device of claim 1 further comprising an antenna for receiving and transmitting messages to and from said contactless smart card.

10. The wireless mobile device of claim 1 wherein said wireless mobile device is selected from a group consisting of a mobile phone, a personal digital assistant, a pager, a wireless laptop computer, a personal computer, a television remote control, and combinations thereof.

11. The wireless mobile device of claim 1 wherein said wireless network is selected from a group consisting of a wireless wide area network (WWAN), a wireless local area network (WLAN), a private network, and a personal area network (PAN).

12. The wireless mobile device of claim 11 wherein said wireless wide area network (WWAN) is selected from a group consisting of a Global System for Mobile Communications(GSM), a Code Division Multiple Access(CDMA), CDMA 2000, and wideband CDMA(WCDMA).

13. The wireless mobile device of claim 1 wherein said wireless mobile device is used for making financial transactions between a user and said entity with said contactless smart card over said network.

14. The wireless mobile device of claim 13 wherein said financial transactions between said user and said entity are face-to-face.

15. The wireless mobile device of claim 13 wherein said financial transactions between said user and said entity are remote.

16. An electronic communication method comprising:

purchasing a good or a service from a merchant; and

paying with a contactless smart card via a wireless mobile device;

wherein said wireless mobile device is adapted to access a wireless network and comprises a subscriber identification module (SIM) card slot and a contactless smart card module electrically connected to said SIM card slot and wherein said contactless smart card module is adapted to receive and read information stored in said contactless smart card and transmit said information to an entity via said wireless network .

17. The electronic communication method of claim 16 further comprising receiving said good or service electronically and storing it in said contactless card.

18. The electronic communication method of claim 14 further comprising retrieving said good or service from said contactless card and redeeming it.

19. An electronic payment method utilized by a customer to pay a merchant with electronic cash stored in a contactless smart card for a face-to-face purchase of a good or service comprising:

placing an order by said customer for said purchase of said good or service to said merchant;

providing a wireless mobile device wherein said mobile device is adapted to access a wireless network and comprises a subscriber identification module (SIM) card slot and a contactless smart card module electrically connected to said SIM card

slot and wherein said contactless smart card module is adapted to receive and read information stored in said contactless smart card and transmit said information via said wireless network;

entering information of said purchase in said wireless mobile phone;

positioning said contactless smart card in close proximity to said wireless mobile device, retrieving smart card identification information and authorizing withdrawal of an electronic cash amount for payment for said good or service from said smart card;

sending said purchase information, said smart card identification information and said electronic cash amount to an authentication server via said wireless network;

authenticating and sending said purchase information and said electronic cash amount by said authentication server to a business account of said merchant held in a financial institution;

registering said purchase information and depositing said electronic cash amount to said merchant's business account and sending confirmation by said financial institution to said authentication server;

forwarding said confirmation to said wireless mobile phone; and

fulfilling said order to said customer by said merchant.

20. An electronic payment method utilized by a customer to pay a merchant with a contactless smart card for a face-to-face purchase of a good or service comprising:

placing an order by said customer for said purchase of said good or service to said merchant;

providing a wireless mobile device wherein said wireless mobile device is adapted to access a wireless network and comprises a subscriber identification module (SIM) card slot and a contactless smart card module electrically connected to said SIM card slot and wherein said contactless smart card module is adapted to receive and read information stored in said contactless smart card and transmit said information via said wireless network;

entering information of said purchase in said wireless mobile phone;

positioning said contactless smart card in close proximity to said wireless mobile device, retrieving smart card identification information from said contactless smart card and authorizing payment for said good or service;

IPR2025-00644 Page 00972

formatting said purchase information, said smart card identification information and said payment authorization into a first message and sending said first message to an authentication server via said wireless network;

authenticating and sending said first message by said authentication server to a financial institution;

registering said purchase information and sending approval for said payment by said financial institution to said authentication server;

forwarding said payment approval to said wireless mobile phone; and

fulfilling said order to said customer by said merchant.

21. The electronic payment method of claim 20 wherein said first message comprises a format selected from a group consisting of Short Message Service (SMS), General Packet Radio Service (GPRS), Transmission Control Protocol/Internet Protocol (TCP/IP), User Datagram Protocol (UDP), Simple Mail Transmission Protocol (SMTP), Simple Network Management Protocol (SNMP), and proprietary message formats.

22. An electronic payment method utilized by a customer to pay a merchant with a contactless smart card for a remote purchase of a good or service comprising:

placing an order by said customer for said purchase of said good or service to a merchant server via a first network and choosing to pay via a wireless mobile device wherein said wireless mobile device is adapted to access a wireless network and comprises a subscriber identification module (SIM) card slot and a contactless smart card module electrically connected to said SIM card slot and wherein said contactless smart card module is adapted to receive and read information stored in said contactless smart card and transmit said information via said wireless network;

providing said merchant server with an identification information for said wireless mobile device;

creating a digital order comprising purchase information and said identification number for said wireless mobile device by said merchant server;

routing said digital order to an authentication server via said first network;

formatting said digital order into a first message wherein said first message is adapted to be transmitted over said wireless network;

routing said first message over said wireless network to said wireless mobile device;

displaying said first message on said wireless mobile device;

requesting and receiving authorization of payment from the customer via said wireless mobile device;

positioning said contactless smart card in close proximity to said wireless mobile device and retrieving smart card identification and security information;

formatting authorization result and smart card identification and security information into a second message and routing said second message to said authentication server;

authenticating and routing said second message to a financial institution, wherein said financial institution is the issuer of said contactless smart card; and

approving and executing said payment at said financial institution.

forwarding said payment approval to said authentication server and from said authentication server to said wireless mobile phone; and

fulfilling said order to said customer by said merchant.

23. The electronic payment method of claim 22 wherein said good or service comprises a digital good or a digital service and wherein said fulfilling comprises downloading and storing said digital good or service in said contactless smart card.

24. The electronic payment method of claim 23 wherein said digital good is selected from a group consisting of electronic cash, electronic coupons, electronic gift certificates, electronic transit tokens,, music, software, movies, and books.

25. The electronic payment method of claim 22 wherein said wireless mobile device is selected from a group consisting of a mobile phone, a personal digital assistant, a pager, a wireless laptop computer, a personal computer, a television remote control, and combinations thereof.

26. The electronic payment method of claim 22 wherein said wireless network is selected from a group consisting of a wireless wide area network (WWAN), a

IPR2025-00644 Page 00974

wireless local area network (WLAN), a private network, and a personal area network (PAN).

27. The electronic payment method of claim 26 wherein said wireless wide area network (WWAN) is selected from a group consisting of a Global System for Mobile Communications(GSM), a Code Division Multiple Access(CDMA), CDMA 2000, and wideband CDMA(WCDMA).

28. The electronic payment method of claim 22 wherein said first and second messages comprise a format selected from a group consisting of Short Message Service (SMS), General Packet Radio Service (GPRS), Transmission Control Protocol/Internet Protocol (TCP/IP), User Datagram Protocol (UDP), Simple Mail Transmission Protocol (SMTP), Simple Network Management Protocol (SNMP), and proprietary message formats.

IPR2025-00644 Page 00975

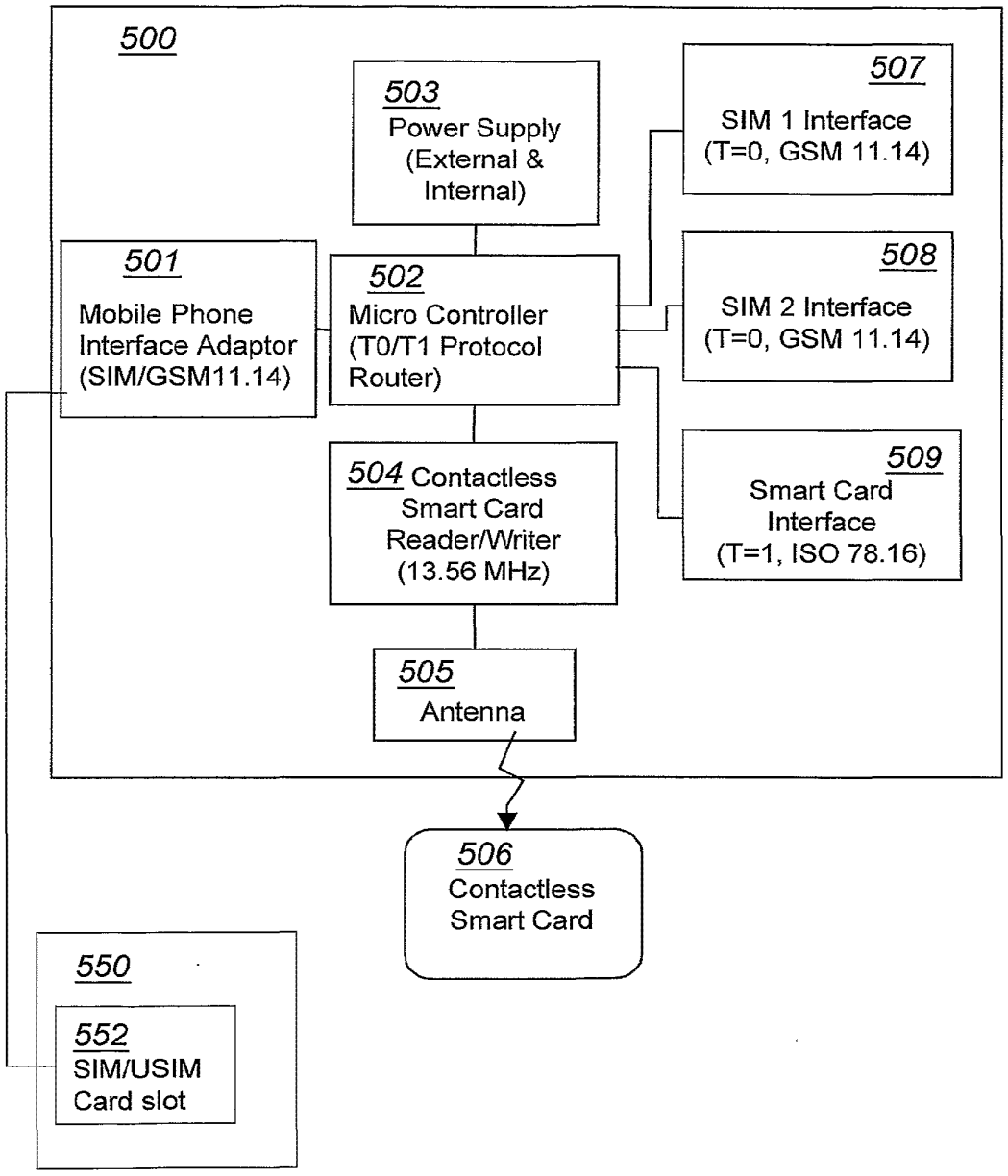

500
503
Power Supply
(External &
Internal)
507
SIM 1 Interface
(T=0, GSM 11.14)
501
Mobile Phone
Interface Adaptor
(SIM/GSM11.14)
502
Micro Controller
(T0/T1 Protocol
Router)
508
SIM 2 Interface
(T=0, GSM 11.14)
504 Contactless
Smart Card
Reader/Writer
(13.56 MHz)
509
Smart Card
Interface
(T=1, ISO 78.16)
505
Antenna
506
Contactless
Smart Card
550
552
SIM/USIM
Card slot

FIG. 1

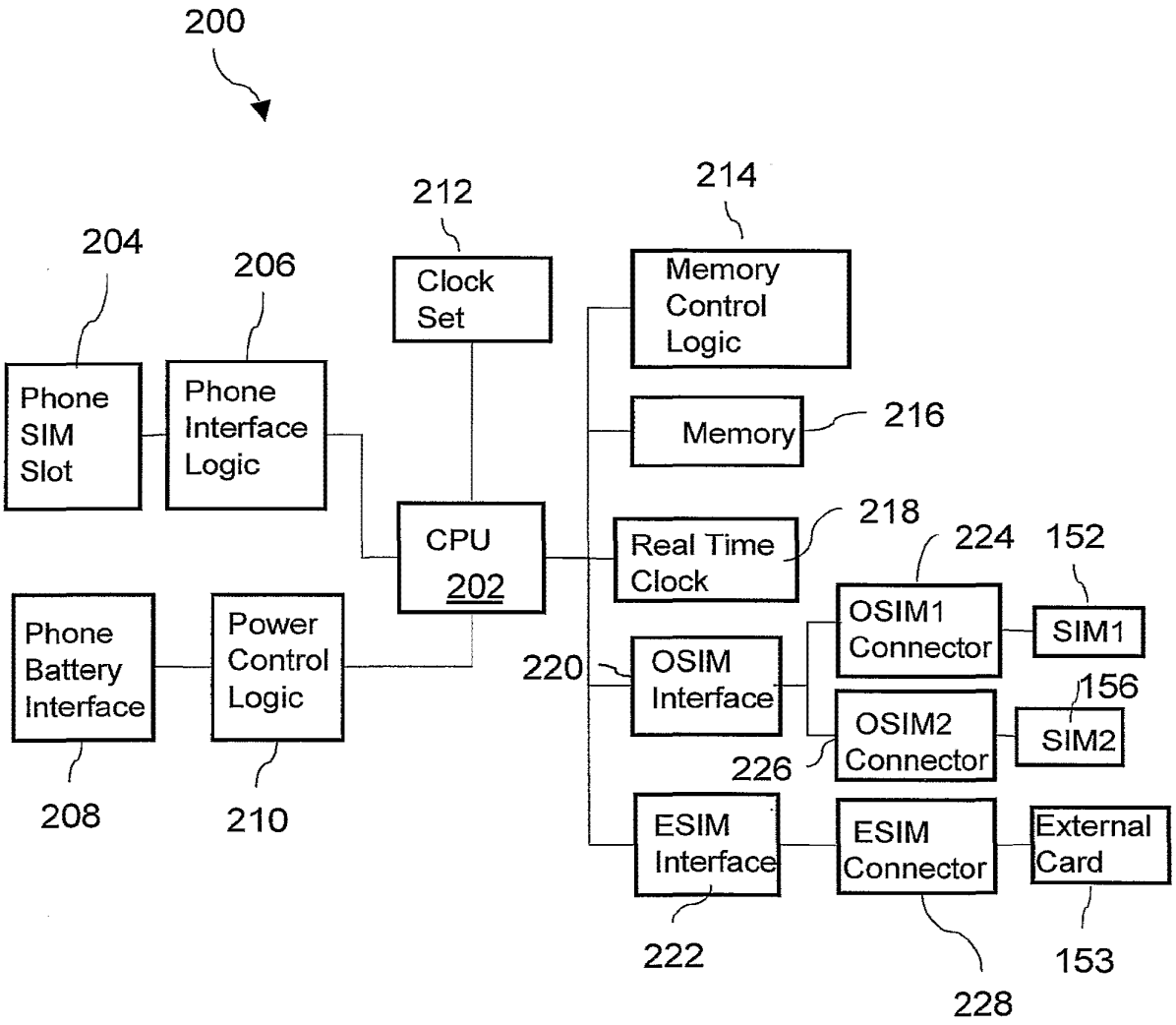

200
212
214
204
206
Clock Set
Memory Control Logic
Phone SIM Slot
Phone Interface Logic
Memory
216
CPU 202
218
224
152
Real Time Clock
OSIM1 Connector
SIM1
220
OSIM Interface
156
OSIM2 Connector
SIM2
226
Phone Battery Interface
Power Control Logic
208
210
ESIM Interface
ESIM Connector
External Card
222
153
228

FIG. 2

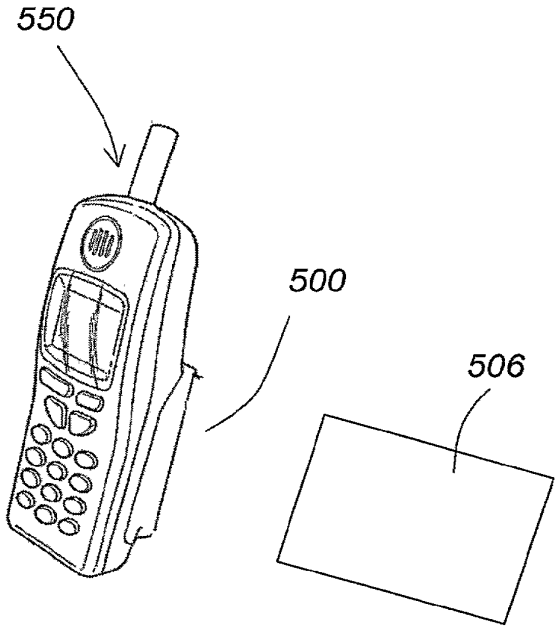


FIG. 3

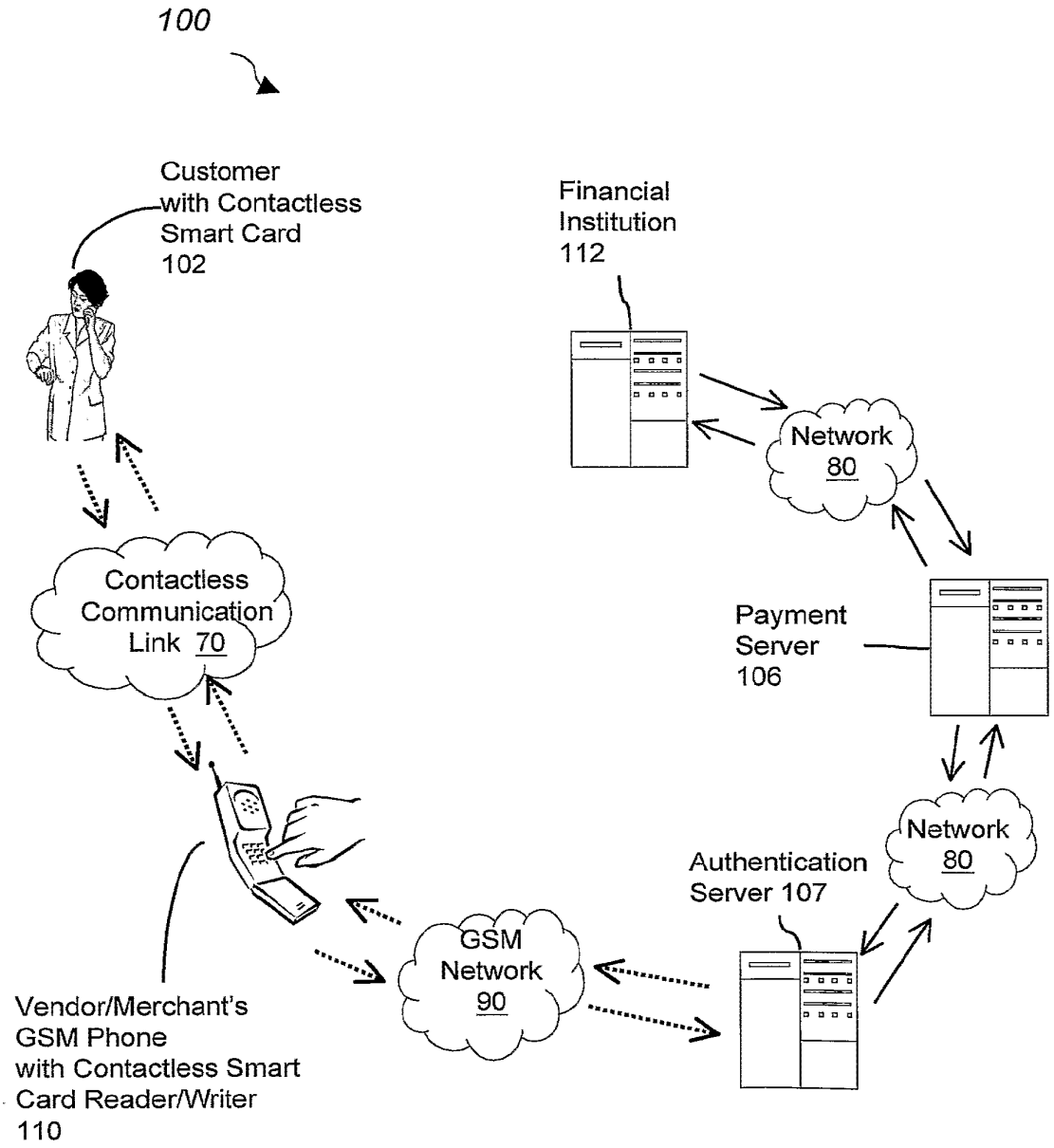

100
Customer with Contactless Smart Card 102
Financial Institution 112
Network 80
Contactless Communication Link 70
Payment Server 106
Network 80
Authentication Server 107
GSM Network 90
Vendor/Merchant's GSM Phone with Contactless Smart Card Reader/Writer 110

FIG. 4

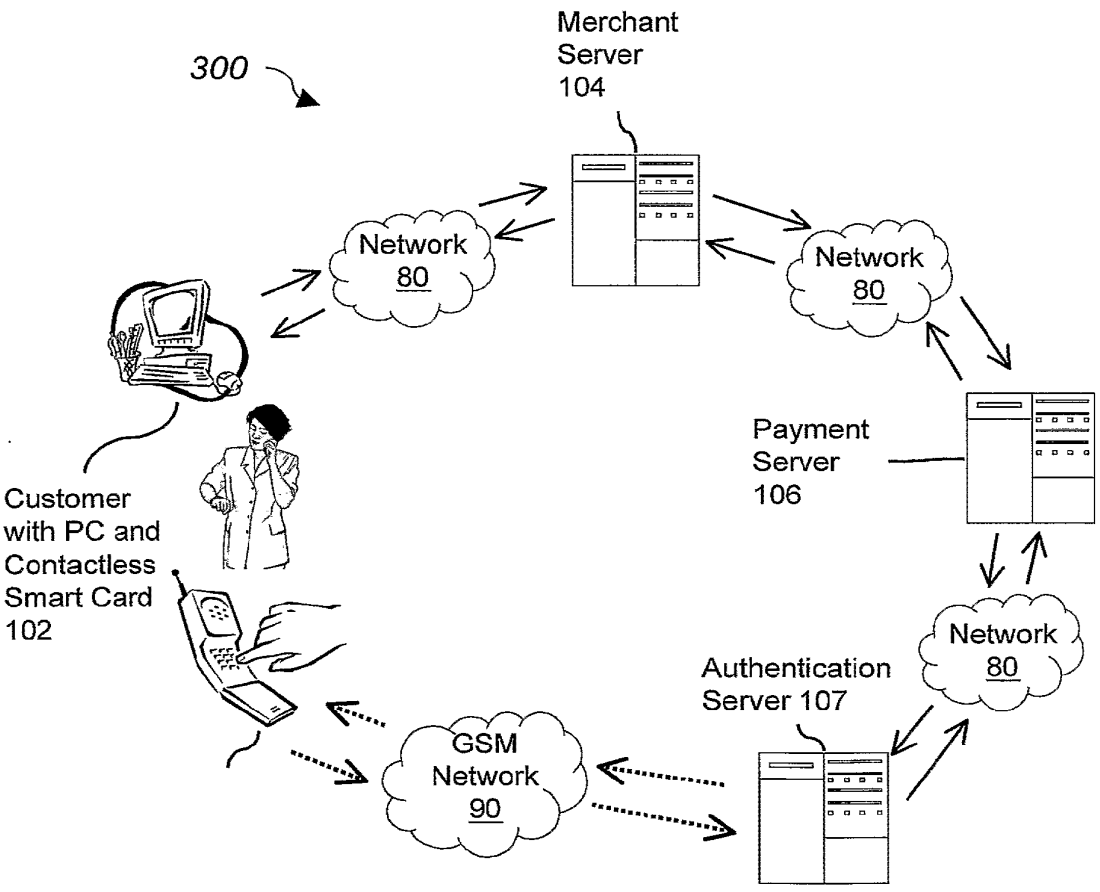

300
Merchant Server 104
Network 80
Network 80
Payment Server 106
Customer with PC and Contactless Smart Card 102
Network 80
Authentication Server 107
GSM Network 90

FIG. 5

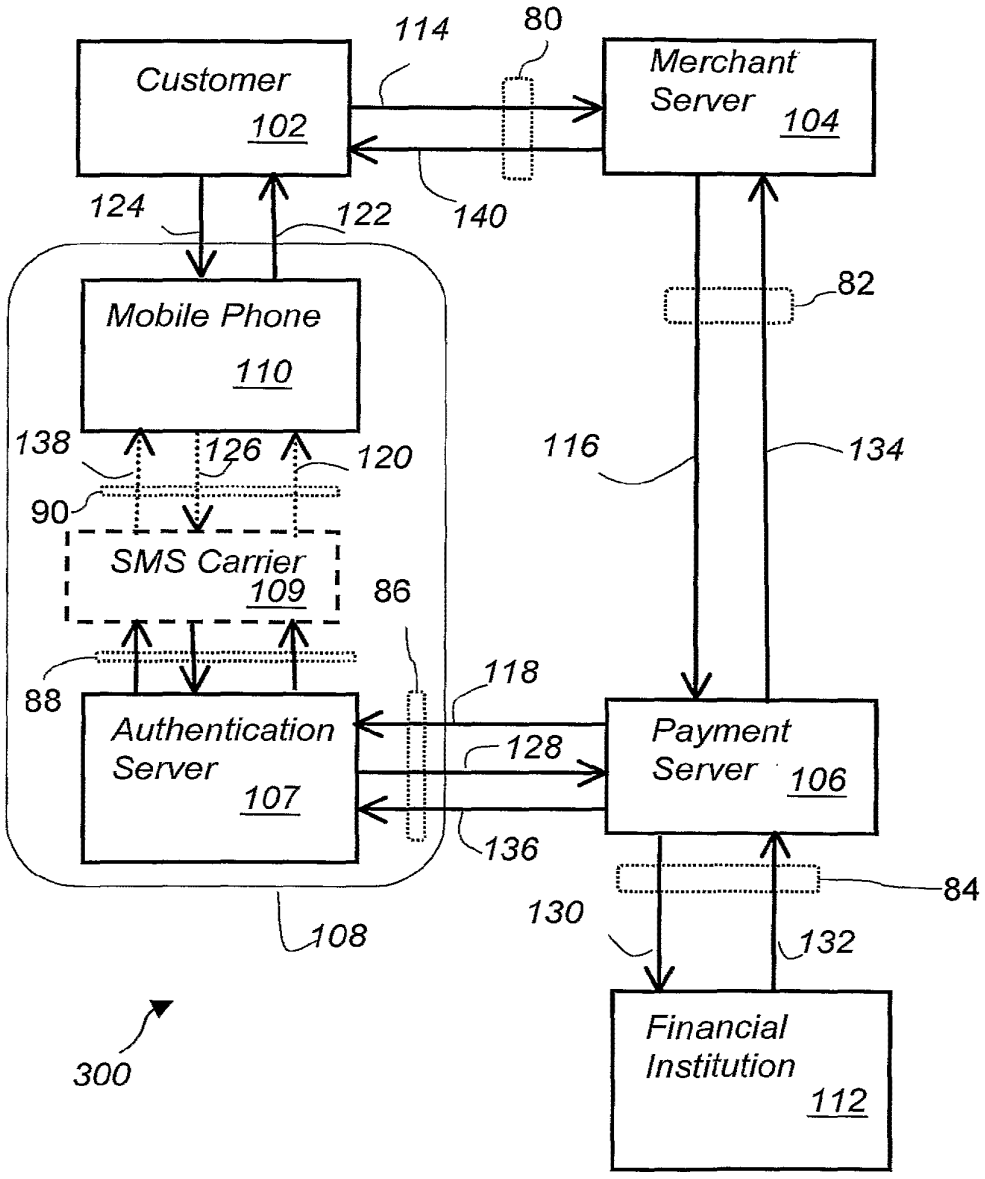

Customer
102
Merchant
Server
104
114
80
140
124
122
Mobile Phone
110
82
138
126
120
116
134
90
SMS Carrier
109
86
88
118
Authentication
Server
107
Payment
Server
106
128
136
84
130
132
108
300
Financial
Institution
112

FIG. 6

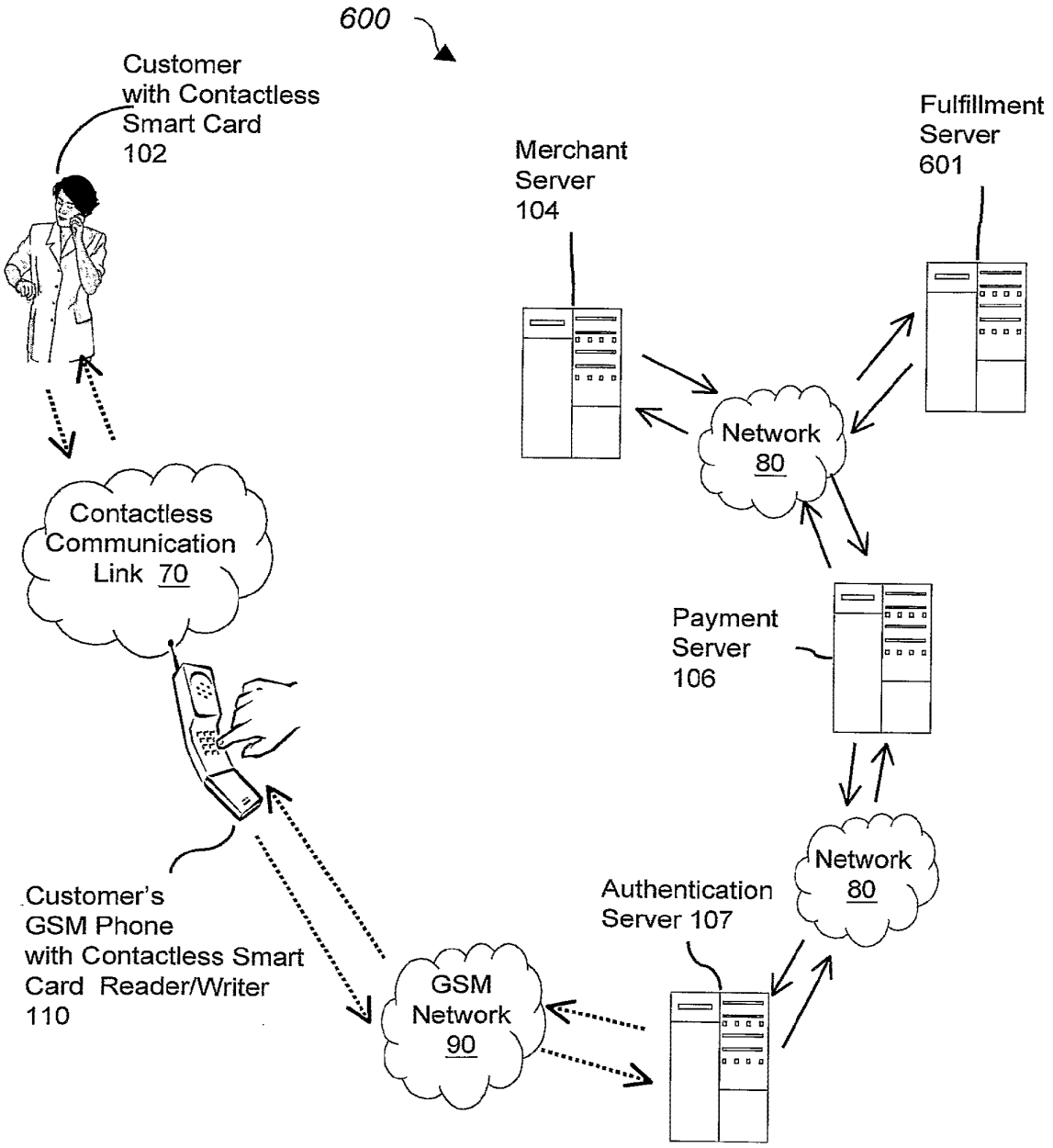

600
Customer with Contactless Smart Card 102
Merchant Server 104
Fulfillment Server 601
Network 80
Contactless Communication Link 70
Payment Server 106
Network 80
Authentication Server 107
Customer's GSM Phone with Contactless Smart Card Reader/Writer 110
GSM Network 90

FIG. 7

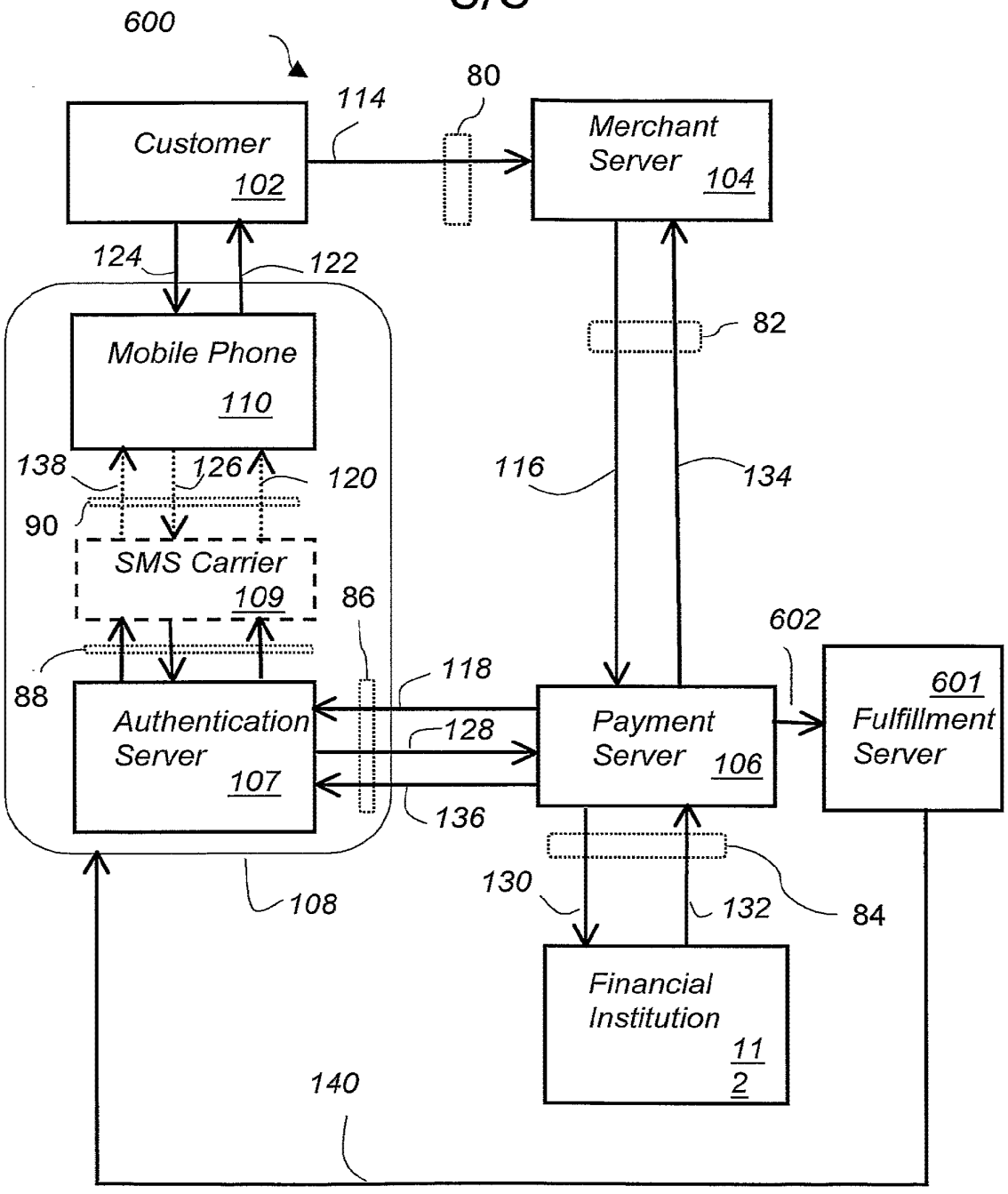

600
Customer
102
114
80
Merchant
Server
104
124
122
Mobile Phone
110
82
138
126
120
116
134
90
SMS Carrier
109
86
602
601
Fulfillment
Server
88
118
Authentication
Server
107
128
Payment
Server
106
136
108
130
132
84
Financial
Institution
11
2
140

FIG. 8

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US03/23080

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) : H04B 1/38
US CL : 455/558, 406-408, 557, 575,550; 705/39, 40, 26; 379/58; 235/380,492

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 455/558, 406-408, 557, 575,550; 705/39, 40, 26; 379/58; 235/380,492

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
None

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
Derwent database.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 2002/0042774 A1 (ORTIZ ET AL.) 11 APRIL 2002, abstract, Fig. 1, Fig. 35-37; [0002, 0024-0025, 0206, 0047, 0088-0089].	1-28
Y	WO 97/46964 A1 (MARTORELL) 11 DECEMBER 1997, abstract, Fig. 7-10; page 14-claim 1; page 5, line 8 to page 6, line 6.	1
Y	US 2002/0002507 A1 (HATAKEYAMA) 03 JANUARY 2002, abstract; [0025]; Fig. 2-steps S11-S13.	1-28
Y	US 6,259,769 B1 (PAGE ET AL.) 10 JULY 2001, abstract; Fig. 1-2; col. 1, lines 7-10; col. 4, lines 28-33; col. 5, line 55 to col. 6, line 2; col. 6, line 13-20; col. 6, lines 39-49.	5-9
Y	US 2001/0034791 A1 (CLUBB ET AL.) 25 OCTOBER 2001, abstract, Fig. 1; [0047, 0056, 0022].	21

☐ 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 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	Date of mailing of the international search report
05 November 2003 (05.11.2003)	03 DEC 2003
Name and mailing address of the ISA/US Mail Stop PCT, Attn: ISA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703)305-3230	Authorized officer Edward Urban Telephone No. (703) 305-4385

Form PCT/ISA/210 (second sheet) (July 1998)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
4 November 2004 (04.11.2004)

PCT

(10) International Publication Number
WO 2004/095169 A2

(51) International Patent Classification[7]: G06F

(21) International Application Number:
PCT/US2004/010951

(22) International Filing Date: 19 April 2004 (19.04.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/464,123 21 April 2003 (21.04.2003) US

(71) Applicant and
(72) Inventor: **OSTERWEIL, Josef** [US/US]; 5411 Amberwood Lane, Rockville, MD 20853 (US).

(72) Inventor; and
(75) Inventor/Applicant *(for US only)*: **SHADMON, Moshe** [US/US]; 4020 Wilkie Way, Palo Alto, CA 94306 (US).

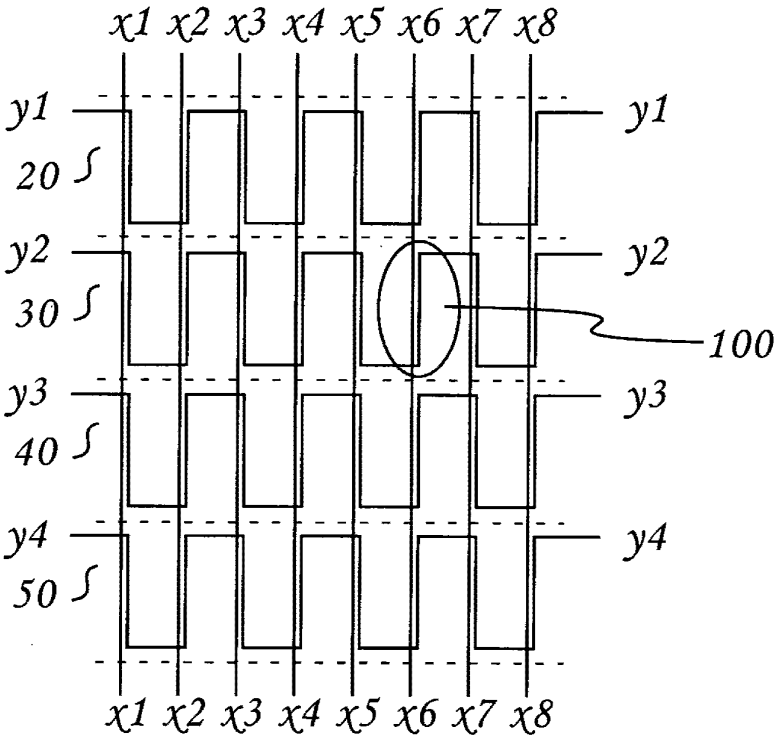
(74) Agent: **OSTERWEIL, Josef**; 5411 Amberwood Lane, Rockville, MD 20853 (US).

(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, 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, TJ, 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).

[Continued on next page]

(54) Title: METHOD AND SYSTEM FOR DATA WRITING/READING ONTO/FROM AND EMULATING A MAGNETIC STRIPE



(57) Abstract: A method of writing data on magnetic stripe of a smart card by imposing a magnetic field of a given polarity on each selected segment of the magnetic stripe, such that data on the magnetic stripe can be read by a magnetic card reader and interpreted as digital bits. The method includes providing a multi-dimensional conductor array placed proximate to the magnetic stripe, the number of conductors in the array is considerably smaller than the number of segments, and each segment is associated with two or more conductors. The method further includes providing current drivers for sending currents in a controlled direction through the conductor array. The system further includes sending currents, using said current drivers, through conductors of the array, such that for each one of the selected segment composite currents flowing through its associated two conductors overcome the coersivity of the segment on the magnetic stripe.

WO 2004/095169 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 AND SYSTEM FOR DATA WRITING/READING ONTO/FROM AND EMULATING A MAGNETIC STRIPE

1. Related Data

[0001] The present application expressly incorporates by reference herein the entire disclosure of U.S. Provisional Application No. 60/464,123, entitled "Method and Apparatus for a data Writing onto and Emulating Magnetic Stripe", which was filed on April 21, 2003.

2. Field Of The Invention

[0002] The present invention is generally in the field of improved smart cards.

BACKGROUND AND RELATED INFORMATION

[0003] The use of plastic cards bearing a magnetic stripe for effecting sales, banking, and other diverse transactions is very popular, in part because of the ease with which such cards may be legitimately used to effect these transactions, and because of the ubiquitous infrastructure that makes their use possible.

[0004] A magnetic stripe on a card enables the card to be swiped repeatedly in a card reader and convey the digital information stored on the stripe to that reader. The information on a magnetic stripe is written onto the stripe by a magnetic write-head, similar to the way digital information is written onto a magnetic tape. Writing onto the magnetic stripe requires that the write-head moves relative to the stripe while generating a variable bipolar magnetic field that represents the data to be stored, and magnetizes the particles along the stripe accordingly. The magnetic stripe material typically in the form of a slurry is deposited on a card, ticket, or other item in a similar way as paint is deposited on a surface. The magnetic particles retain the memory of their last direction of the magnetic polarity until a magnetic field strong enough to overcome the particle's coercive force changes the polarity to a new direction.

[0005] The American National Standards Institute (ANSI) & ISO/IEC has defined standards relating to magnetic stripe cards.

[0006] A typical magnetic stripe is segmented into four channels, three of which are defined for a specific format by ANSI. These tracks are defined only by their location on the magnetic stripe. Each is dedicated to a different purpose:

Track one contains the cardholder's name as well as account and other discretionary data

Track two contains the cardholder's account number, encrypted Personal Identification Numbers (PIN), finger print characteristics, and other discretionary data. This track is the most commonly used and is read by Automatic Teller Machines (ATM) and credit card checkers

Track 3 is unique and rarely used.

[0007] Most ATM cards follow these standards, but there are many other types of cards (key cards, security cards, copy machine cards, etc.) that do not follow these established standards.

[0008] Smart cards refer to cards that typically include embedded input/output interface, memory, and a microprocessor. Smart cards look like standard plastic cards, but are equipped with embedded Integrated Circuit(s). Smart cards can store information, execute local processing on data, and interface with external devices. These cards take the form of either "contact" cards that require an electrical connection to an external card interface (Card Acceptance Device (CAD)) or "contactless" cards that communicate by electromagnetic signals to the external card interface (CAD). The contact card typically has eight metallic interface pads on its surface, each designed to international standards for VCC (power supply voltage), RST (used to reset the microprocessor of the smart card), CLK (clock signal), GND (ground), VPP (programming or write voltage), and I/O (serial input/output line). Two pads are reserved for future use (RFU). Only the I/O and GND contacts are mandatory on a card to meet international standards; the other contacts are optional.

[0009] When a smart card is inserted into a Card Acceptance Device or CAD (such as a point-of-sale terminal), the metallic pads come into contact with the CAD's corresponding metallic pins, thereby allowing the card and CAD to communicate. Smart cards are reset when they are inserted into a CAD. This action causes the smart card to respond by sending an "Answer-to-Reset" (ATR) message, which informs the CAD of what rules govern communication with the card and the processing of a transaction.

[0010] Note that in the context of the invention, smart cards are not bound to the structure and manner of operation discussed above. Thus, for example, contact smart cards are not bound by the particular standard described above, and this applies also to contactless cards. By way of another example, smart cards are not bound by any specific substrate, such as plastic cards.

[0011] Notwithstanding the advantages of smart cards over magnetic cards, the adoption of smart cards has been relatively slow in the US and other leading markets. One of the main reasons for their slow adoption is the present lack of support infrastructure (e.g. dedicated readers), necessitating retrofitting of equipment such as vending machines, ATMs, and telephones to incorporate dedicated readers that are adapted to read smart cards and possibly also write data thereon.

[0012] The standard "non-smart" magnetic stripe cards, on the other hand, enjoy a ubiquitous infrastructure in many commercial, access control, and other applications and notwithstanding their inferiority compared to smart cards, consumers use predominantly magnetic cards.

[0013] The invention according to the PCT publication WO 01/88659 (hereinafter the PCT publication) combines the inherent advantages of smart cards with the widely circulated magnetic card readers. PCT WO 01/88659 discloses an electronic card that can function as an anonymous credit card or banking card for use on or off the Internet, and which utilizes a magnetic storage medium affixed to the card that can be read by a standard magnetic stripe reader. An encoder generates a data packet that can be stored in a designated portion of the magnetic storage medium, which can be a magnetic stripe. The data packet can contain a personal coupon and an alias. A computer or microprocessor generates the personal coupon after a Personal Identification Number is input into the card. The data packet can also be used to convey other information, such as a low battery condition. Several different methods of customizing use of the electronic card provide a vast array of options for handling multiple users, bills, and accounts; and for characterizing individual transactions of the card.

[0014] The device disclosed in the '659 publication offers backward compatibility in the sense that information stored in or generated by the smart card and stored in track #2 of the magnetic stripe is accessible by conventional magnetic card readers. The backward compatibility allows the users and industry to benefit from the widely circulated and reliable infrastructure of the magnetic cards readers, and obviates the need for extensive and expensive retrofit, as would be required with conventional smart cards using dedicated smart card readers.

[0015] Some of the principles of operation which relate to the PCT application, and which serve as a background for understanding the invention, will be explained with

reference to Figs. 1 to 3. Fig. 1 shows current flowing through a conductor 4 (illustrated in cross-section front view in Fig.1) that generates magnetic field 6 of strength H (around the conductor 4). The strength of the magnetic field H complies with the following algorithmic expression:

$$H = \frac{I}{R}$$

[0016] Where: I is the current in the conductor and R is the radius (distance) from the center of the conductor 4 to the location of interest where magnetic field 6 H is measured. The direction of the magnetic field 6 H is clockwise as indicated by the arrows on the magnetic field lines 6, and corresponds to a current direction in the conductor 4 that is perpendicular to the page and flows in a direction from the viewer into the page.

[0017] As is further shown in Fig. 1, a thin magnetic stripe layer segment 2 is located in close proximity to the conductor 4. The flow through the conductor imposes a magnetic field with polarity of North Pole (N) and South Pole (S), as indicated in Fig.1. The SN poles illustrated in Fig.1 constitute a magnetic domain; each track in the magnetic stripe layer includes a plurality of magnetic domains in a line. When the current direction is reversed in a direction from the page to the viewer, the direction of the magnetic field is reversed to counterclockwise, and so are the S and N polarities on the magnetic stripe (not shown). The magnetic field strength 6 must be intense enough to overcome the coercivity of the magnetic stripe 2 material. Since the magnetic field is proportional to the current in the conductor 4, it is necessary to reach a balance between the magnitude of the current pulse and the coercivity of the magnetic material. Once the magnetic polarity on the magnetic stripe 2 has been set by the current, the current flow can be stopped and the imprint on the magnetic stripe will remain in that setting until reversed by a reverse current in the conductor 4 or by an external magnetic field that is strong enough to overcome the coercivity of the magnetic stripe 2. Thus, current impulses of the right magnitude and direction are sufficient to imprint data on the magnetic stripe material.

[0018] Note that it is desirable to minimize the magnitude of the current pulses so that currents and their current drivers become manageable. However, the lower the coercivity of the magnetic stripe material, the more susceptible is the magnetic stripe to

being inadvertently modified by external magnetic fields.

[0019] Fig.2 illustrates a typical card 10 with a magnetic stripe and four channel (tracks) 20, 30, 40, and 50. The resolution of such a magnetic stripe varies and some standards suggest 75 and 210 bits per inch of data density.

[0020] Fig. 3a shows a schematic view of a segment of one channel of the associated magnetic stripe 70 of a smart card. Items 80a, 80b, and 80c, drawn in dotted lines, represent the conductors in a layer below the magnetic stripe 70. Note that the distance between the conductors determines the maximal bit density possible. For example, for a resolution that will accommodate 210 bits per inch, at least 210 conductors per inch must be constructed.

[0021] Fig.3B illustrates a cross-section view along AA of the segment depicted in Fig. 3A, in which 80a, 80b, and 80c are the conductors with insulating material 75 between them, while on top of them is located the magnetic stripe 70.

[0022] Fig.3C illustrates a cross-section view along BB of the segment depicted in Fig. 3A in which the leads 82a and 82b are made available for connections between the conductor 80c and a current delivery and switching drivers.

[0023] The principles described with reference to Figs. 1 to 3 above are suitable for integration with a smart card. The current drivers deliver the currents necessary to write and rewrite the data content of the smart card's magnetic stripe, in accordance with the conceptual approach described with reference to Fig. 1. The smart card's direct writing is initiated by external command inputs to the smart card or by, for example, stroke(s) on the card's keyboard. After having written the data on the magnetic stripe, when the smart card is swiped in a standard magnetic stripe reader, the last data written will be available to the reader.

[0024] To summerize, Fig. 3A, Fig. 3B and Fig. 3C, track # 2 of magnetic stripe 70 is part of a standard credit card, and the conductors 80a, 80b, and 80c as well as the insulator 75 are part of the smart card (as described in the PCT publication).

[0025] There are also provided appropriate electronics and current drivers. The object bearing the magnetic stripe 70, for example, a credit card is placed in close proximity to the conductors 80a, 80b, and 80c as seen in Fig. 3b, all forming part of the card. Currents through the conductors 80a, 80b, and 80c induce the data information onto the stripe.

[0026] A smart card of the kind described generally in Figs. 1 to 3 is disclosed in the '659 PCT publication but it purports only to offer an improved smart card which facilitates digital data transformation into a format that is compatible with the standard magnetic stripe reader. One of the significant disadvantages of the smart card disclosed in the '659 publication is the use of a many conductors and a cumbersome electronic system including current drivers in order to facilitate data writing onto the magnetic stripe. Such a cumbersome electronic system (as will be explained with greater detail below) poses high manufacturing costs and consumes battery power, thereby hindering the wide circulation into the marketplace of a smart card of the kind disclosed in the '659 publication.

[0027] For a better understanding of the cumbersome structure of the electronics system and drivers in accordance with the PCT publication, there follows a description of a "write bit" operation (of bit value '0' or '1'), including flip bit value (from '1' to '0' or vise versa) and "read bit" operation.

[0028] Thus, and as depicted in Fig. 7D of the '659 publication (attached herewith and marked as 3D), each bit is represented by two magnetic domains (each being imposed to either SN or NS magnetic orientation). As may be recalled, the description with reference to Fig. 1, above, exemplified the correspondence between current flow direction in the conductor and corresponding magnetic orientation (SN or NS) per domain.

[0029] As depicted in Fig. 7D, each domain is associated with two conductors, which, depending upon the direction of the currents flowing through the respective conductors (e.g. 34 and 35 of Fig. 7D), will impose the polarity of the magnetic domain to NS or SN (using basically the concept described in Fig. 1, above).

[0030] Generally speaking, when the current flows in a prescribed direction through the two conductors associated with a given magnetic domain (say 34 and 35 in Fig. 7D), it imposes a polarity NS. Similarly, the polarity of the mating magnetic domain is also imposed to NS (using current flowing in the same prescribed direction through its respective two conductors). Given two successive NS domains written in the manner specified current direction, (i.e. the polarity of each one of the mating magnetic domains is imposed to NS), when a conventional magnetic reader reads the succession of NS and NS (i.e. the neighboring magnetic domain have the same magnetic orientation), there is

no flux reversal (i.e. the magnetic reader regards the two consecutive domains as a single NS), and thus indicates a bit value of '0'. Similarly, when the magnetic card reader reads a succession of SN and SN (where, during a preceding writing phase, each SN was imposed on a magnetic domain by current flowing in prescribed direction through the respective two conductors associated with the magnetic domain), it also indicates a bit value of '0', since here also there is no flux reversal. In contrast, when the magnetic orientation of a first magnetic domain is SN and the magnetic orientation of the neighboring domain is opposite (NS), the magnetic reader senses flux reversal between the neighboring domains, and this is interpreted as '1'. By the same principle two opposite magnetic orientations NS followed by SN, will likewise give rise to flux reversal (sensed by the reader) and will be interpreted as '1'.

[0031] The encoding of '0' and '1' in the manner specified is illustrated in Fig. 7B of the PCT publication (attached herewith and marked as 3E) where, as shown, consecutive domains with identical magnetic orientation (NS, NS or SN, SN) are interpreted as '0' (see, for example, the first raw of the specified Fig. 7B), whereas consecutive magnetic domains with opposite magnetic orientation (NS, SN or SN, NS) are interpreted as '1'. Note that the frequency of '1' (e.g. the second raw of Fig. 7B) is twice the frequency of the '0' (e.g. the first raw of Fig. 7B), in accordance with the *Aiken Biphase* code discussed in the PCT publication.

[0032] In accordance with the PCT publication, two conductors are used per domain, giving rise to four conductors per each bit. The use of two conductors per domain and associated electronics, as described in the '659 publication, facilitates relatively rapid writing and changing of current flow direction (through the conductor(s)) whenever flipping polarity is required (i.e. when a bit value needs to be inversed from '1' to '0' or vise versa). This writing and flipping polarity is achieved at the cost of using a cumbersome system that includes 4 conductors and associated electronics per bit. The associated electronics include current drivers that employ one transistor per conductor. Considering that a relatively high current is required to overcome the magnetic coercivity of the magnetic domain (whenever flipping the polarity is required), the so utilized transistor should sustain currents of relatively high magnitudes, requiring thus power transistors which consequently require larger real-estate on the board or silicon chip than low current transistors do.

[0033] As may be recalled, relatively high currents are utilized since the higher the current, the stronger the generated magnetic field, thereby reducing the prospects of undesired flipping of the magnetic domain's polarity due to influence of external magnetic fields.

[0034] Thus, for example, for a series of 500 bits that reside on the magnetic stripe, 2000 conductors and 2000 power transistors (used in the current drivers) are utilized. The description with reference to Fig. 8 of the 659 publication illustrates the complexity of a system of the kind specified.

[0035] Realizing such a cumbersome system in a chip that is incorporated in a card having dimensions of a conventional credit card is relatively expensive, because the conductors and associated electronic circuitry would require relatively large real-estate chip space, rendering the manufacture of such chips expensive. Note also that the more complicated the chip, the lesser the yield rate (i.e. the percentage of the fault free manufactured chips), giving rise to increased manufacturing costs, chip price, and the resulting smart card.

[0036] Note also that circuitry of the kind specified consumes battery power (due to the use of many current drivers, thus significantly reducing the lifespan of the card's battery, posing undue burden of the user who is compelled to frequently change or re-charge used batteries.

[0037] Note also that the switching mechanism of pulsed current in selectable directions into each individual conductor embedded in the magnetic stripe has been used in prior art in conjunction with, for example, magnetic core memory, and will therefore not be further expounded upon herein.

[0038] It is thus appreciated that the solution according to the '659 publication suffers from various shortcomings; accordingly there is a need in the art to provide for a novel backward-compatible solution of a smart card that can be used, *inter alia*, with conventional magnetic card readers. Such an improved smart card can be used, among other uses, to consolidate a plurality of credit cards into a single smart card.

[0039] There is a further need in the art for providing an improved smart card capable of static emulation of magnetic stripe, for use with conventional magnetic card readers.

[0040] There is still further need in the art for providing an improved smart card capable of dynamic emulation of magnetic stripe, for use with conventional magnetic

card readers. There is still further need in the art to use such improved smart card in dual function, allowing also writing thereto using conventional magnetic card writer.

[0041] There is still further need in the art for providing a new type of magnetic card writer with no moving parts, configured to write data on magnetic stripes of conventional credit cards, for example.

SUMMARY OF THE INVENTION

[0042] In accordance with a first aspect of the invention, there is provided a smart card device that includes processing and other means coupled to storage medium, and which is associated with a magnetic stripe. The processing and other means enable direct writing of information onto the magnetic stripe. The so written data is originally stored in the storage of the smart card, and/or is generated by the processor of the smart card, and/or based on information that has been received from external source (e.g. by the user through input means such as a keypad that is associated with the smart card).

[0043] In accordance with an embodiment of the first aspect of the invention, there is provided an improved smart card accommodating a stationary bi-dimensional or multi-dimensional array, such as bi-dimensional matrix, without moving parts that selects writing (current flow) to each conductor by addressing at least two matrix coordinates utilized by the smart card. This matrix simplifies the complexity of the electronic drivers that inject current into each conductor segment. As will be explained in greater detail below, such reduced complexity leads to certain advantages, including reduced manufacturing and retail costs, as well as extending the product's battery lifespan.

[0044] There is provided, in accordance with a first aspect of the invention, a method of writing data on magnetic stripe of a smart card by imposing magnetic field of a given polarity on each selected segment of the magnetic stripe, such that data on the magnetic stripe can be read by a magnetic card reader, and interpreted as digital bits, comprising:

(i) providing a multi-dimensional conductor array placed proximate to the magnetic stripe, where the number of conductors in the array is considerably smaller than the number of segments, and where each segment is associated with at least two conductors;

(ii) providing current drivers for sending currents in controlled direction through the conductor array; and

(iii) sending currents, using said current drivers, through conductors of the

array, such that for each one of the selected segment composite currents flowing through it's associated segment in at least two conductors overcome the coersivity of the segment of the magnetic stripe.

[0045] There is thus provided, in accordance with a second aspect of the invention, a method for statically emulating a magnetic stripe, such that data can be read by a magnetic card reader and interpreted as digital bits, comprising:

a) providing in a smart card a conductor array proximate to the card's surface;

b) providing current drivers for sending currents in controlled direction through the conductor array; and

c) sending currents, using said current drivers, through conductors of the array, for generating magnetic field of sufficient magnitude so as to be read by the magnetic card reader and interpreted as digital bits, while the card is being swiped for reading.

[0046] In accordance with a third aspect of the invention there is provided a dynamic emulation of a magnetic stripe that facilitates motionless card reading. In accordance with this aspect, the smart card is positioned so that the magnetic field generated by the conductor is proximate to the magnetic read-head of a card reader. In accordance with this aspect, there is no need to swipe the card such that the magnetic stripe (or the magnetic field in case of static emulated magnetic stripe) traverses the read head of the reader. Accordingly, errors that stem from undue swiping of the card (and which occasionally require that the user should re-swipe the card) are avoided. As will be explained in greater detail below, in dynamic emulation the number of conductors is significantly reduced and the associated electronics is considerably simplified. The net effect is that manufacturing costs are significantly reduced and the smart card's battery lifespan is considerably extended.

[0048] There is thus provided in accordance with a third aspect of the invention a method for dynamically emulating a magnetic stripe, such that data can be read by a magnetic card reader and interpreted as digital bits, comprising:

(i) providing at least one conductor proximate the card surface;

(ii) providing at least one current driver for sending current through the at least one conductor; and

(iii) sending variable current, using at least one said current driver, through the at least one conductor, for generating magnetic field of sufficient magnitude so as to be read by the magnetic card reader and interpreted as digital bits.

[0048] There is still further provided, in accordance another aspect of the invention, the use of a conventional magnetic stripe writer for conveying data to the smart card using the magnetic coupling between the write head and (possibly) an elongated conductor(s).

[0049] There is thus provided in accordance with this aspect of the invention a method for writing data onto a smart card, using a magnetic card writer, comprising:

a) providing at least one conductor proximate the card surface; and

b) providing a magnetic coupling between the write head of a magnetic stripe writer and at least one conductor, for entering data to the smart card.

[0050] Still further, there is provided in accordance with another aspect of the invention a new type of magnetic writer, with no moving parts. The magnetic writer includes a conductor array that is external to the card and is used as a magnetic stripe writer for writing onto standard magnetic stripe cards.

[0051] There is thus provided in accordance with this aspect of the invention a method for writing data on a magnetic stripe of a magnetic card, comprising:

(i) providing a conductor array proximate to the magnetic stripe;

(ii) providing current drivers for sending currents in controlled direction through the conductor array; and

(iii) sending currents, using said current drivers, through conductors of the array, for generating magnetic field of sufficient magnitude so as to overcome the coersivity of the magnetic stripe.

[0052] The invention further provides for a system for writing data on a magnetic stripe of a card, comprising a writing device capable of writing data onto the magnetic stripe being placed in proximity thereto, such that the writing device is characterized as having no moving parts.

[0053] The invention further provides for a system for writing data on a magnetic stripe of a card, comprising a writing device capable of writing data onto the magnetic stripe dynamically, in conjunction with a device synchronizing it to the swipe velocity of the card.

[0054] Still further, the invention provides for a smart card storing information of multiple cards such that the said card includes a processor and an associated device capable of conveying data indicative of a selected card from among said plurality of cards to a magnetic stripe of the smart card, so as to be read by a magnetic card reader.

[0055] Still further, the invention provides for a smart card storing information of multiple cards such that the said card includes a processor and an associated device capable of emulating data indicative of a selected card from among said plurality of cards such that said emulated data is capable of being read by a magnetic card reader.

[0056] Still further, the invention provides for a system of storing data indicative of multiple cards in a storage area of a programmable module; such that the said system is capable of transferring data to a magnetic stripe of a card.

BRIEF DESCRIPTION OF THE DRAWINGS

[0057] For a better understanding, the invention will now be described, by way of example only, with reference to the accompanying drawings, in which:

Fig. 1 illustrates a cross-section front view of a conductor and related magnetic field for illustrating the principles of magnetism, electric current, and the relationship between them;

Fig. 2 illustrates schematically an exemplary card with four channels and associated magnetic stripe;

Fig. 3A illustrates a schematic view of a segment of one channel of an associated magnetic stripe in a smart card;

Fig. 3B illustrates a cross-section view along AA of the segment depicted in Fig. 3A;

Fig. 3C illustrates a cross-section view along BB of the segment depicted in Fig. 3A;

Fig. 3D illustrates a structure of magnetic domains forming part of a smart card, in accordance with the prior art;

Fig. 3E illustrates a representation of encoded sequences of bits, in accordance with prior art Aiken Biphase encoding standard;

Fig. 4A illustrates a matrix conductor array in accordance with an embodiment of an aspect of the invention;

Fig. 4B illustrates a matrix conductor array example of a single track layout,

in accordance with an embodiment of an aspect of the invention;

Fig. 4C illustrates yet another matrix conductor array example of a single track layout, in accordance with an embodiment of an aspect of the invention;

Fig. 4D illustrates a conductor dynamic magnetic stripe writer example with a synchronizing device to the swipe velocity, in accordance with an embodiment of an aspect of the invention;

Fig 5A illustrates a schematic view of a segment of one channel of a magnetic stripe in a smart card, in accordance with an embodiment of an aspect of the invention the invention;

Fig. 5B illustrates a cross-section view along AA of the segment depicted in Fig. 5A;

Fig. 5C illustrates a cross-section view along BB of the segment depicted in Fig. 5A;

Fig. 6 illustrates a cross-section front view of a conductor and related magnetic field, which will serve in understanding the operation of certain embodiments of an aspect of the invention;

Fig. 7 illustrates a cross-section front view of a conductor and related magnetic field, which will serve in understanding the operation of certain embodiments of an aspect of the invention;

Fig. 8A illustrates a schematic view of a segment of one channel, in accordance with an embodiment of an aspect of the invention;

Fig. 8B illustrates a cross-section view along AA of the segment depicted in Fig. 8A;

Fig. 8C illustrates a cross-section view along BB of the segment depicted in Fig. 8A;

Fig. 9 illustrates schematically an exemplary card with four channels, in accordance with an embodiment of an aspect of the invention;

Fig. 10 illustrates a signal waveform in a coil for generating corresponding flux, as a function of time, where the flux is aimed at the read head of a standard magnetic stripe reader, in accordance with an embodiment of an aspect of the invention;

Fig. 11 illustrates a conductor for use in a smart card, in accordance with an embodiment of the invention;

IPR2025-00644 Page 00999

Fig. 12 illustrates a view of a coil with a C-shaped core, relative to the read head of a standard magnetic stripe reader, in accordance with an embodiment of an aspect of the invention;

Fig. 13 illustrates schematically an exemplary card with four channels, in accordance with an embodiment of an aspect of the invention;

Fig. 14 illustrates a view of a coil with a C shape core relative to the write head of a standard magnetic stripe writer, in accordance with an embodiment of an aspect of the invention;

Fig. 15A illustrates a schematic view of a segment of one channel of the magnetic stripe writer and proximate magnetic stripe card, in accordance with an embodiment of an aspect of the invention;

Fig. 15B illustrates a cross-section view along AA of the segment depicted in Fig. 15A;

Fig. 15C illustrates a cross-section view along BB of the segment depicted in Fig. 15A;

Fig. 16 illustrates a generalized sequence of operation of transferring data, in accordance with an embodiment of the invention; and

Fig. 17 illustrates schematically modules of a smart card, in accordance with an embodiment of the invention.

DETAILED DISCLOSURE OF THE INVENTION

[0058] Fig. 17 illustrates schematically modules of a smart card in accordance with an embodiment of the invention.

[0059] In accordance with a first aspect of the invention, there is provided a bi-dimensional or multi-dimensional conductor array that is proximate to the magnetic stripe that copes with the shortcomings of the hitherto known solutions. Fig. 4A illustrates a non-limiting embodiment of this aspect of the invention utilizing a matrix conductor array. It should be noted that the invention is not bound by any specific magnetic material that forms the magnetic stripe.

[0060] Thus, as shown, two substantially proximate conductors are associated to each domain, to allow a selection of each domain by the sum of currents in the two conductors. (As may be recalled, two domains constitute a single bit). Therefore, the sum of two currents flowing in the same direction is designed to overcome the coercivity

of the magnetic stripe for each domain, whereas each current alone or two opposing currents will not. In Fig. 4A, current through lines y2-y2 and x6-x6 that add together to become a higher current at domain 100 is an example of such matrix domain selection. This approach is akin to the selection process of a single core in a magnetic core memory, allows the selection to be accomplished in the form of a matrix, and consequently uses fewer current drivers. Note that in the context of the invention, domain is only one example of a segment of a magnetic stripe that is subjected to imposition of magnetic field, for writing data thereon. The invention is not bound by this example.

[0061] Fig. 4B illustrates a matrix conductor array example of a single track layout in accordance with an embodiment of an aspect of the invention. Fig. 4B further clarifies how the matrix approach can be laid out in a single track. Note that the specific single track layout of Fig. 4B (of x1-x8 over y1-y4 matrix) corresponds to the schematic matrix representation of the same x1-x8 over y1-y4 depicted in 4A.

[0062] The example illustrates the connecting links 101 between successive sets of domain conductors corresponding to x1 – x8 and y1 –y4, respectively. Note that these links 101 are perpendicular to the domain active conductors, and therefore have no impact on the data content. For example, the domain active conductors Y2 and X6 that control domain 100 are normal to links 101, and therefore currents flowing through links 101 have substantially no impact on the magnitudes of the currents flowing through X6 and Y2 conductors at location 100. Note that in the layout of Fig. 4B, each of the X and Y conductors (by this particular example, 4 and 8, altogether 12) have a square waveform-like shape, and that active conductor segments of each *i,j,* conductors (e.g. the conductors segments 100 that are associated with their domain) are placed proximate and substantially parallel to the domain (the domain is not depicted in Fig. 4B).

[0063] Note that in order to further reduce any registration of the links on the magnetic stripe material, these links can be placed on the back layer of the matrix substrate.

[0064] Those versed in the art will readily appreciate that the invention is not bound by the specific layout depicted in Fig. 4B.

[0065] Utilizing a conductor array in accordance with the embodiment of Fig 4 constitutes a significant advantage over the conductor arrangement offered in the '659

PCT publication, in that it requires considerably lesser number of conductors and simpler associated electronics. Thus, a matrix having A rows and B columns can support up to A * B entries, i.e. bits. For instance, in the case of 500 bits, 1000 domains are required and, thus, a 32 over 32 matrix can be employed such that any one of the 1000 domains (or up to 1024 domains) is controlled by a unique (i,j) entry. Accordingly, 64 lines are required to write any desired bit in the series of 500 bits. Even if each entry is implemented by using 2 conductors (i.e. 2 conductors per domain, similar to the solution offered by the '659 PCT application) in order to facilitate inversion of current flow direction, still, a total of 64 * 2, i.e. 128 conductors are utilized compared to 2000 as was the case in the invention according to the '659 publication. Obviously, simpler associated electronics are required, e.g. fewer current drivers are required. Moreover, note that in order to write a bit value in location (i,j), the sum of the currents flowing through entry i and entry j should be high enough to overcome the coercivity of the magnetic domain that corresponds to the (i,j) bit. This necessarily entails that the current through each entry is of lesser intensity than the total current required overcoming the magnetic domain coercivity. Considering the lower current flow through each entry, this requires use of current drivers of lower power. Thus, this embodiment offers use of considerably fewer conductors, with simpler associated electronics that includes considerably fewer transistors, each of which support lower current. This necessarily entails that the a chip that accommodates the conductors and the associated electronics in accordance with this embodiment has considerably lesser manufacturing costs and, due to the lesser number of conductors, current drivers and the lower current intensity, it lowers the cost and complexity of each driver compared to that provided in accordance with that of the 659 publication.

[0066] Note that the invention is not bound by the specified matrix realization. Thus, for example the matrix is not necessarily confined to identical number of rows and columns. The current flowing through each entry is likewise not necessarily identical. In other words, it is not necessarily required to push half current intensity through the line entry and another half current intensity through the columns entry in order to bring about a full current intensity required to overcome the coersivity of a magnetic domain. By way of example, 0.75 intensity may be driven through the row entry and 0.25 intensity through the column. Of course, other variants are applicable as required and

appropriate. Note that, when using non-identical currents, a careful design should avoid undesired scenarios in which one of the currents is too close to be able to overcome the coersivity. For example, having one current with 0.98 intensity and the other current with 0.02 appears to be risky, because in certain operational scenarios the 0.98 intensity current can overcome by itself the coersivity. The same consideration should apply to the utilization of non identical current in three-dimensional or greater matrix, as will be explained in greater detail below.

[0067] By way of another example, a three-dimensional matrix is employed, thus reducing even more the number of conductors that are used. For example, for 500 bits (or 1000 domains) a X * Y * Z matrix can be used with, 10 lines per dimension (supporting up to 1000 domains) giving rise to 30 (i.e. 10*3) lines. Even if using a bi-directional current switch on a single wire, such that two conductors are used (one for each current direction in accordance with the approach of the PCT publication), a total of 60 lines are required (i.e. 30*2), instead of 128 lines, as in the case of two-dimensional matrix exemplified above.

[0068] Another matrix example is illustrated in Fig. 4C. This matrix is two-dimensional and reduces the number of necessary drivers in the same manner as the matrix described in Figs 4A and 4B. However, the objective of this example is to emphasize a minimum number of conductors per bit. Consequently, a single conductor will be driven with enough current to overcome the coersivity of the magnetic stripe material, where the drivers y3 and x4 selectively drive conductor element 100. All drivers in this example are bidirectional and drive current in the direction dictated by the data content. The importance of this matrix example is for cases where the technology reaches yield degradation at the range of high conductor densities (more than one conductor per 5 mils).

[0069] Other bi-dimensional or multi-dimensional conductor array arrangements that are not necessarily confined to matrix configuration are applicable, all as required and appropriate.

[0070] Note that the invention is not bound by the specific architecture illustrated in Fig. 4A through 4C, in which the conductor array (being in accordance with one embodiment of the invention in the form of a matrix of conductors) is located below the magnetic stripe layer.

[0071] The matrix form can be effectively used as a standard magnetic stripe card writer, as will be shown later. These magnetic stripe card writers are static in the sense that there are no moving parts. Fig 4D shows a simple magnetic stripe writer that implements dynamic write conductor elements (320, 330, 340, and 350 shown one for each of the four tacks). These conductors and a swipe velocity synchronization device are mounted on a substrate 300 against which the card 110 is swiped. The card 110 has a longitudinal reference 302 that is read by the synchronization device. The synchronization device reads a linear location of the magnetic stripe, which is used to control the dynamic write rate of the conductor write elements. The linear reference can be best obtained optically, but other media is not precluded. Adjustment for the write conductor elements for air gap and intertrack leakage will be accomplished as necessary using ferromagnetic materials.

[0072] The conductor elements 320, 330, 340, and 350 are each driven by current that corresponds to the respective track data, as illustrated in Fig. 10 for example. The current generates a corresponding magnetic field as is the case in standard magnetic stripe write heads. As the card is being swiped the data segments are distributed along the track(s). The synchronization of the data rate to the swipe velocity ensures that the data is correctly distributed along the track(s).

[0073] In accordance with the invention, Figs 5A, Fig. 5B and Fig. 5C representing another example arrangement of magnetic stripe and conductors. The arrangement according to Figs. 5A-C is similar to Figs. 3A-C, except that the magnetic stripe material 70 is in the layer underneath and between the conductors. The results are very similar to the first embodiment except that the resulting polarity is reversed, as evident in Fig. 6.

[0074] Those versed in the art will readily appreciate that the various embodiments discussed above are only few out of many exemplary configurations of a conductor array proximate to the magnetic stripe material for the purpose of writing data onto the magnetic stripe, in accordance with the first aspect of the invention.

[0075] In accordance with a non-limiting application of an improved smart card (described, for example, with reference to the first aspect of the invention), a single smart card can substitute the function of multiple magnetic stripe cards (serving thus as a multi-card) and allow the user to easily change the card's identity/function using the smart card's input/output interfaces, such as a built-in keyboard or display. In other

words, a single smart card can store data indicative of plurality of magnetic cards (say of many credit cards) and whenever the card holder wishes to use a given magnetic card, the appropriate data (corresponding to the magnetic card of interest) is written onto the magnetic stripe and can be read by conventional magnetic card reader. The invention is, of course, not bound by this application.

[0076] In accordance with a second aspect of the invention, and as will be explained in greater detail below, there is provided a static emulation of a magnetic stripe by current magnitude and direction control in a conductor retained for the duration of the reading of the emulated magnetic stripe, where the generated magnetic field should substantially correspond to the mapping of bits on a magnetic stripe, in accordance with the standard. Note that the magnetic stripe material is absent, as its functionality is being emulated.

[0077] For a better understanding of the second aspect of the invention, Fig. 6 illustrates how a conductor 104 generates a magnetic field 106 at the air gap 108 where the direction of the magnetic field 106 H is clockwise, as indicated by the arrows on the magnetic field lines 106, and corresponds to a current direction in the conductor 104 that is perpendicular to the page and flows in the direction from the viewer into the page. Note that, generally, the operation in accordance with Fig. 7 is similar to that of Fig. 1, except for the fact that in the latter the magnetic field is generated on the magnetic stripe. As will be explained in greater detail below, using a magnetic field generated at the air gap would facilitate use of lower currents, thereby further simplifying the associated electronics and extending battery lifespan.

[0078] Fig. 7 illustrates how a conductor 104 that is partially surrounded by ferromagnetic material 102 generates a magnetic field 106 at the air gap 108, with the North Pole (N) to the left and the South Pole (S) to the right of the conductor 104. The use of ferromagnetic material that partially surrounds the conductor (compared to free air that entirely surrounds the conductor, as is the case in Fig. 6), intensifies the magnitude of the magnetic field generated at air gap 108. It should be noted that the invention is not bound by any specific type of ferromagnetic material and not by the specific geometry as illustrated in Fig. 7. For example, the sector size of the ferromagnetic material and/or the geometrical shape thereof may vary depending upon the particular application.

[0079] Bearing all this in mind, Fig. 8A, illustrates a schematic view of a segment of one channel, in accordance with an embodiment of the second aspect of the invention.

[0080] In accordance with this embodiment there is provided a static magnetic stripe emulation, obviating the need of using magnetic stripe material. By this embodiment, an array of conductors 180a, 180b, and 180c, shown in Figs 8A-C are embedded in a nonconductive material 170 proximate the surface of the smart card's enclosure, and spaced corresponding to the data poles on the emulated magnetic stripe. The conductor array is designed such that it will generate the magnetic field in the air at an area that corresponds to the channel tracks, e.g. 20, 30, 40, and 50 of the magnetic stripe in Fig. 2. Current flowing in each of these conductors in directions that correspond to the data bits being emulated, generate a magnetic field in the air (as was described with reference to Fig. 6) along each track such that they can be read by a magnetic stripe reader. Note that because the magnetic field generated need only be read by a sensitive read head of the magnetic stripe reader, it is not required to overcome the coersivity of magnetic stripe material (as was the case with the embodiments in accordance with the first aspect of the invention as well as the prior art 659 publication) because the currents required are very low. By way of non limiting example, in certain embodiments in accordance with first aspect of the invention, the current flowing through each conductor is of the magnitude range of about 300 $mA - 1A$. In contrast, in accordance with certain embodiments of the second aspect of the invention, the current flowing through each conductor is of the magnitude of about 1 mA. The specified magnitudes are mentioned for illustrative purposes and are by no means binding.

[0081] In operation, the user indicates the specific card that is to be used (say, VISA™ credit card), including PIN and/or finger print to identify an authorized user. In response, the processor retrieves from the storage (both forming part of the credit card) data indicative of the VISA™ credit card. In the case that the storage stores data indicative of a plurality of credit cards, the data indicative of the sought VISA™ credit card is identified and retrieved. This operational scenario is by no means limiting and other examples are illustrated by way of non limiting examples with reference to Figs. 16 and 17, below. Now, when the user swipes the card in the reader, the processor controls the current flow through the array of conductors to generate a magnetic field with S/N polarity that corresponds to the data bits of the emulated VISA™ credit card.

By one embodiment, the conductor array and the associated electronics (for writing a bit value of '0' or '1') are similar to that of the 659 publication. In accordance with another embodiment of the second aspect of the invention, a matrix array configuration (of the kind described in detail with reference to the first aspect above) may be employed, thereby reducing the number of conductors and their associated current drivers, all as discussed in detail above.

[0082] Note that the static emulation must operate when the card is swiped through the card reader. The emulation can commence shortly before or simultaneously with the swiping of the card through the reader, and the emulation can end when the data is properly read, or shortly after the card has been swiped through the reader. The emulation can likewise be achieved when the current in the conductors is applied sequentially, provided that the sequencing rate is not impacting normal swipe rates. The start/stop of emulation can be automatic or by a user initiated command.

[0083] The use of low currents constitutes an advantage, as compared to the use of high currents, because the associated electronics (including the power drivers) is considerably simpler (e.g. transistors compared to power transistors), giving rise to smaller real-estate chip space and consequently lower manufacturing costs. Moreover, utilizing lower currents gives rise to longer battery lifespan. As may be recalled, in accordance with the second aspect of the invention, currents are sustained during the reading process. The reading process may be interrupted by the existing external magnetic fields (due to the lower currents that are used) and, accordingly, if desired, higher currents may be employed, all depending upon the particular application.

[0084] In accordance with a third aspect of the invention, there is provided a dynamic emulation of a magnetic stripe by the current's magnitude control and its direction in a conductor. The current's polarity changes in accordance with the data and at a rate determined to be appropriate for a typical magnetic stripe reader. This constitutes a variable magnetic field burst, corresponding to the data to be delivered to the magnetic stripe reader, which is repeated, if necessary, at least for the duration of the reading of the emulated magnetic stripe.

[0085] An embodiment of the third aspect of the invention is based on a dynamic emulation of a magnetic stripe, and obviates the act of swiping. Fig. 9 illustrates an embodiment of a smart card 110 in which the four track (channel) magnetic stripe has

IPR2025-00644 Page 01007

been substituted with four electromagnetic transducers such as sections of conductors 120, 130, 140, and 150 surrounded by ferromagnetic material, as shown in Fig. 7, or in accordance with another embodiment without the ferromagnetic material (as shown in Fig. 6) . Note that in Fig. 6, the air surrounding the conductor is used for illustrative purposes only. In practice a material that will have no substantial effect on the magnetic field (such as non Ferromagnetic material) is used to surround selected sectors of the conductor. Note also that the invention (in accordance with the third aspect) is not bound by specific configurations of Figs. 6 and 7.

[0086] In operation, the card is placed in a conventional magnetic stripe reader in a manner that brings the conductors 120, 130, 140, and 150 proximate to the reading head of the reader. The smart card emulates the swiping action of a magnetic stripe by generating the same varying magnetic field as that of a magnetic stripe being swiped in the vicinity of the read-head. The varying magnetic field is induced by an electromagnetic transducer and is controlled by the transducer's driver in the direction and intensity of the current. For four magnetic stripe channels, four such transducers 120, 130, 140, and 150 and drivers are used. Note that the conductors have to be placed *vis-à-vis* the reader and, if reading does not occur, i.e. the conductors are displaced relative to the read head, the magnitude of the magnetic field sensed by the magnetic head reader may be too low. In this case the user will have to repeat the procedure until the data is successfully read.

[0087] For a better understanding of the foregoing, refer to Fig. 10 which illustrates current polarity in a conductor for generating corresponding flux as a function of time, where the flux is aimed at the read head of a standard magnetic stripe reader, in accordance with an embodiment of an aspect of the invention. The current is driven to the coil, and the resulting flux corresponds directly in amplitude and direction to the current generating it. Note, that in the signal illustrated in Fig. 10, the frequency of the '0' is half that of the '1', which is in compliance with the Aiken Biphase encoding standard, giving rise to appropriate interpretation of the '0' and '1' bits by a standard magnetic reader. The generation of a signal of the kind depicted in Fig. 10 is generally known *per se,* and therefore will not be further expounded upon herein.

[0088] The invention is, of course, not bound by this particular Aiken Biphase encoding scheme.

[0089] Note that the rate of change of the current, and consequently the flux, represents the swiping action of a standard card. The baud rate (the reciprocal of the shortest time between two sequential transitions i.e. equivalent to one domain being swept) of the data stream being generated by the smart card can be set to any value desired, within the rate range set by the standards. Typically, although not necessarily, it should be set to a safe value around the middle of the range. Once set, it will be consistently repeated every time the card is used, with drifts confined to the tolerance of the internal card's clock.

[0090] The baud rate of data generated by the write head of the magnetic stripe card writer is determined by the manufacturer of the magnetic stripe card writer. The smart card will synchronize to that rate in a similar fashion as a magnetic stripe card reader synchronizes to the data baud rate determined by the swipe velocity of the card. The format of the data transfer is specified in great detail in the standards. The standard includes a preamble of zeros for synchronization. However, custom format outside the specifications of the standards (which is often necessary for track 3) are possible.

[0091] In accordance with certain embodiments of this aspect of the invention, it is possible to employ a single conductor per track, and to feed through the conductor variable currents indicative of the series of bits that are normally accommodated in a credit card track (say, 500 bits, as described in the examples above), as depicted, for example, in the description with reference to Fig. 10. Note that, similar to the second aspect of the invention, the dynamic emulation, in accordance with the third aspect, can take place substantially during the use of the card, and need not be activated when the card is not in use, thereby saving power consumption.

[0092] The invention in accordance with this aspect constitutes a significant advantage in that only few conductors are used and, accordingly, a very simple associated electronics circuitry is required to drive currents to the conductors. This exhibits even greater current savings and further reduces the number of current drivers, compared to the static emulation, in accordance with the second aspect of the invention (the latter, as may be recalled, constitutes a significant current savings over hitherto known solutions). The current consumption in accordance with the third aspect of the invention is reduced because the data is presented sequentially, i.e. in certain embodiments no more than one bit is generated at a time, compared to all the bits

generated simultaneously, in accordance with certain embodiments of the second aspect of the invention.

[0093] Note also that by this embodiment of the third aspect of the present invention, the card can be placed in a selected stationary position inside the reader, thereby obviating the need to swipe the card in the reader. This may constitute an advantage for users who are unable to swipe the card rapidly in the reader (e.g. those suffering from motoric disorders), and now find it unnecessary to perform repeated attempts to swipe the card until the data is duly read by the reader. What would be required in accordance with this embodiment is simply to place the card inside the reader (preferably, although not necessarily, in the center), and the data will be conveyed to the reader by means of the dynamic emulation described above.

[0094] By another embodiment of the third aspect of the invention, a magnetic field representing the data extends along a longer segment of the smart card, mimicking the same location where a standard magnetic stripe would be placed. Fig. 11 illustrates a single track of elongated magnetic field generated by an electromagnetic transducer, such as a solenoid/coil 260 (constituting an elongated conductor) that functions substantially equivalent to multiple conductors of the kind depicted in Fig. 6. The current flowing through the elongated conductor flows in the same direction as that which flows through the equivalent multiple of conductors. The resulting magnetic field 206 can be adjusted to certain boundaries by the use of ferromagnetic material, as at least one of a core of the solenoid/coil and external to the solenoid/coil. The ferromagnetic material can be used to isolate magnetically one track from another, and the material is placed between the coils. This may be necessary to separate the magnetic fields of two adjacent tracks. The utilization of the magnetic material in the manner specified can be, e.g. (but not limited to) in accordance with the teachings of techniques used for magnetic flux control and electrical shielding.

[0095] For a better understanding of the operation of the embodiment of Fig. 11, attention is drawn to Fig. 12, which illustrates an example of how information is transferred between a coil 260a using a C core 212a and a typical read head 214a in a magnetic stripe reader. A current passed through the coil 260a using the coil terminals 208a and 210a results in flux 206. The direction of the flux 206 varies in accordance to the current direction in the coil 260a, e.g. according to the exemplary pattern described

above with reference to Fig. 10. Note that the current is driven into the coil terminals 208a and 210a. The air gap 215a of the read head 214a of the reader is positioned in the path of the flux 206 and, as a result, a corresponding data signal is induced on the read head's coil terminals 216a and 218a, which is subsequently processed by the magnetic stripe reader's electronics (not shown). Ferromagnetic materials such as metal, ferrite, etc., as well as electrical shielding techniques, can be used to fine tune the path of the flux for optimal performance.

[0096] Fig. 13 illustrates schematically a four track (channel) 220, 230, 240, and 250 smart card 110 that utilizes an elongated conductor of the kind depicted in Figs. 11 and 12. Note that, if desired, the elongated conductor does not necessarily extend through the entire track and, accordingly, by way of another embodiment, the elongated conductor is replaced by two or more shorter conductors that are placed side by side.

[0097] By the embodiment described with reference to Figs. 11 to 13, the card can be placed in the reader in a motionless manner (as was the case with the embodiment described with reference to Fig. 9); however, considering that the elongated conductor provides the same information throughout its longitudinal extent, the card can be placed substantially at any stationary position inside the reader, thereby obviating the need to swipe the card in the reader. This may constitute an advantage for users who are unable to swipe the card rapidly in the reader (e.g. those suffering from motoric disorders) and now find it unnecessary to perform repeated attempts to swipe the card until the data is duly read by the reader. What would be required in accordance with this embodiment is simply to place the card inside the reader and the data will be conveyed to the reader by means of the dynamic emulation described above.

[0098] If desired, the card can be swiped in the conventional manner. This is because the elongated conductor provides the same information throughout its longitudinal extent while the card is swiped.

[0099] Attention is now drawn to Fig. 14, which illustrates an embodiment in accordance with another aspect of the invention. By this embodiment, the elongated conductor (e.g. that described with reference to Fig. 12, above) is used to transfer data from a standard magnetic card writer to the smart card. In other words, a conventional magnetic stripe writer conveys data to the smart card using the magnetic coupling between the write head and the elongated conductor.

[0100] In operation, a magnetic flux 219 emanates from the conventional magnetic write head 214b. The magnetic flux corresponds to the current direction to the write head's coil terminals 216b and 218b. The flux 219 is sensed by the C core 212b and the coil 260b, resulting in data signals at the coil terminals 208b and 210b. By following this approach, data is written to the smart card, using a conventional magnetic write head. Using a standard magnetic write head for writing data to a smart card is not limited to the specific implementation described with reference to Fig. 14.

[0101] As may be recalled, hitherto known techniques for writing data into smart cards employ transmitting data through designated interface pin(s) for contact smart cards, or communicating by electromagnetic signals from external card interface for contactless cards. In accordance with this aspect of the invention, there is provided yet another means for writing data to smart cards, using standard magnetic write head. As explained above, with reference to the third aspect of the invention, the smart cards that are used are simple, inexpensive, and consume very low power, thereby constituting advantage over other known smart cards.

[0102] By a modified embodiment, a read/write functionality is provided, where the smart card of the kind described in a non limiting manner with reference to Figs. 11 and 12 is used with a standard magnetic head reader for reading data of interest, (e.g. VISA™ credit card data stored therein), and using a standard magnetic write head, new (or modified) data can be written onto the smart card, using, for example, the technique described in a non-limiting manner, with reference to Fig. 14.

[0103] Thus, for example, this embodiment also allows a conventional magnetic stripe writer to convey data to the smart card using the magnetic coupling of the write head with the four track channel transducers 220, 230, 240, and 250 (see Fig. 13). These transducers are compatible with a conventional magnetic stripe reader and writer for two-way data transfer to and from a smart card.

[0104] Still further, there is provided in accordance with another aspect of the invention a new type of magnetic stripe card writer, with no moving parts. The new type of writer includes a conductor array being external to the card and used as a magnetic stripe writer onto standard magnetic stripe cards..

[0105] Attention is now drawn to Figs. 15A, 15B, and 15C, which illustrate an example of a new generation of magnetic stripe card writer, in accordance with an

embodiment of the invention. The magnetic stripe card 370 is placed against the conductor array block 375 (showing conductors: 380a, 380b, and 380c only) where the magnetic stripe 371 faces the array. The card is aligned with the array (using appropriate restraining means), so as to have each track of the magnetic stripe face its corresponding conductor array section. The air gap 372 between the magnetic stripe 371 and the array block 375 is kept to a minimum for best transfer of data. The currents in the conductor array must overcome the coersivity of the magnetic stripe material. The array currents in the conductor array may be applied simultaneously or sequentially (one domain is magnetized at a time) without substantially affecting the data transfer onto the magnetic stripe of the card.

[0106] By another embodiment, instead of using an array of conductors in the manner described with reference to Fig. 15, a bi-dimensional or multi-dimensional array of conductors is used, similar as in the various embodiments described with reference to the first aspect of the invention. A non-limiting example being a bi-dimensional matrix, described with reference to Figs. 4A-B above. The use of matrix of the kind specified simplifies manufacturing and reduces costs, as compared to the use of array of conductors of the kind described with reference to Fig. 15.

[0107] As explained above, the invention in accordance with various embodiments thereof obviates the need to carry multiple magnetic cards by storing the content of the multiple cards in a single physical card. It further offers better fraud protection to the consumer. The description below refers mainly to an application of consolidating multiple (magnetic) cards in a single smart card (or programmable device, such as cellular telephone or PDA, referred to also as multi card application). The invention is not bound by this application. For instance, it may be used for other applications, such as those disclosed in the PCT publication.

[0108] Thus, the data indicative of the multiple cards can be stored on the smart card, which accommodates also a processor, and in response to user selection, the data of selected card is conveyed by means of the processor through the conductors to the magnetic stripe or emulates the magnetic stripe, all as described in detail above.

[0109] By another embodiment of the invention, a portable programmable device stores the information of the multiple cards, and in response to user selection, the data of selected card is conveyed to the magnetic stripe of a conventional magnetic card (or

emulates the magnetic stripe), all as described in detail above. The programmable device forms part of external device such as, for instance, a PDA or cellular telephone fitted with or coupled to a writer of the kind described above, e.g. with reference to Fig. 15. The cellular telephone fitted with or coupled to a writer of the dynamic kind of Fig.4D or a standard magnetic stripe writer is another embodiment possible.

[0110] Note that by one embodiment, the user does not have a smart card, but rather a conventional, generic magnetic card, which is updated with appropriate data (e.g. of the selected credit card) from the external programmable device being for example the user's PDA or cellular telephone.

[0111] The data indicative of the cards (say the credit cards) can be transferred to the smart card (in the case it holds the data indicative of multiple cards), or to the programmable device (in the case it holds the data indicative of multiple cards) from an external source through either direct or remote coupling, using a safe communication channel.

[0112] When the user wants to select a given card to use (from among the plurality of stored credit cards), there is provided in accordance with one embodiment an interactive module that presents to the user a summary of the information stored (such as names of the cards, total spending of each card from a specific date etc.), and allows the user to pick the card, using input means such as keypad. The interactive module can form part of the smart card or the programmable device, depending upon the particular application.

[0113] In order to store data of existing cards, their contents is read (using, say conventional magnetic card reader), and the data is stored in the smart card/external programmable device for later use. Optionally, additional information can be added by the user through an optional interactive module. The additional data being, for example, the type of the card (e.g. credit / debit card), credit limits, amount spent from a particular date, the card distributor, and any other information that might be of interest to the user.

[0114] By one embodiment, the smart card has an embedded display presenting information relating to the emulated card. The display can optionally present the visible information that exists in the original magnetic card, e.g. the contents of each or selected track. Such information can include the name of the institution that supplies the card, the card number, the name of the holder, expiration date, and a sample signature.

IPR2025-00644 Page 01014

[0115] A non-limiting example of a display that can be used is a Ferroelectric LCD that does not require power to maintain the current contents of a display, as it only requires power to change the displayed contents.

[0116] By another non-limiting example, the display is powered by the smart card's power. Other variants are applicable.

[0117] In accordance with an embodiment of the invention, the user can use the smart card only if he or she enters a PIN through the interactive module. The use of PIN can be required, e.g. before commencing a transaction, or once a day, or once a week at any other time, or not required at all. Certain protection means can be employed, e.g. the insertion of a wrong PIN would delete the content (or portion thereof) of the card. Alternatively, N consecutive failures to insert the correct PIN would delete the content (or portion thereof) of the card. Other variants are, of course, applicable.

[0118] By one embodiment of the invention, a provider (say the credit card operator, such as VISA™, MASTERCARD™, etc. transmits information to the programmable device (say a cellular phone), and the latter is capable to receive and store transmitted information. The information is then transferred to the card via the card writer that either forms an integral part of the programmable device, or is coupled thereto.

[0119] Non-limiting examples of such transmitted information are:

- The information needed to activate a card.
- The information needed to configure a new card.
- The information needed to complete a transaction.

[0120] If desired, the transmission of data can be secured by a PIN, finger print reader, and/or other encryption means. In accordance with this embodiment, the user is exempted from accessing the bank to receive a new card when the previous one has been expired, because the updated data can be transmitted from the credit card operator in the manner described above. Note, generally, that in the context with the various aspects of the invention, encryption means encompass PIN, finger print detection, voice recognition (being example of biometrics identification), and/or other known *per se* means.

[0121] Attention is now drawn to Fig. 16, which illustrates a generalized sequence of operation of transferring data, in accordance with an embodiment of the invention. The invention is, of course, not bound by this specific example.

[0122] Thus, module "A" is a programmable module allowing operation with a card reader and/or writer, designated "B", in order to transfer the information to a smart card designated "C".

[0123] Module "A" receives card information read from the magnetic stripe of one or multiple cards using module "B" as a card reader (or possibly other dedicated reader). The information is stored in a storage area of module "A". If desired, additional (user defined) information is added to the information stored within module "A" by input means, such as a keypad that is coupled to module "A". By one embodiment, module "A" is an integral module in the smart card "C".

[0124] By another embodiment, module "A" forms part of a programmable device, such as cell-phone, capable of receiving keyed-in and/or transmitted information and/or magnetic card information read from a magnetic card reader. This information is stored or added to the storage area of module "A". In operation, the information is transferred to magnetic card "C", via the writer functionality of module "B" (the latter can be separated from A or being integral part thereof). The writing of data to magnetic card C can be, for example, in accordance with the procedure described with reference to Fig. 15.

[0125] As described above, the user can interact with module "A" via a keypad and LCD screen. The user is able to view some or all of the stored cards' information, decides which information to send to the magnetic card, and initiates the transfer of the information to the magnetic card.

[0126] In the case that modules A and B are fitted in a smart card, the data can be written to the magnetic stripe of the smart card or be sent to emulate the magnetic stripe, all as described in detail above with reference to the various aspects of the invention.

[0127] Attention is now directed to Fig. 17, which illustrates a configuration process of the smart card, in accordance with an embodiment of the invention. The invention is of course not bound by this example.

[0128] In the Fig. 17, the module designated "A" is a smart card incorporating the following modules:

Module "B" is a LCD device. Module "C" is data storage area. Module "D" is a keypad device. Module "E" is the magnetic stripe of said smart card. Module "F" is a processor running a control program capable of interacting with the keypad "D", data

IPR2025-00644 Page 01016

storage "C", LCD "B", the magnetic stripe "E", and module G. Module G is a conductor array and associated electronics, as described above with reference to various aspects of the invention.

[0129] By this non-limiting example, information of three cards (numbered 1, 2, and 3) is stored in the storage area "C". The control program "F" is initiated by a user interaction with the keypad "D", to navigate between the information of the different cards. Thus, program "F" switches between the information of the cards 1,2,3 in response to user interaction through keypad "D". Whenever program "F" switches between cards' information, program "F" sends some of the information of the current card to the LCD "B". This information is, e.g., the card name and number (that is presented on the original card). The user is able to select the card of interest, according to the displayed data, by invoking instructions via the keypad "D", and thus program module "F" sends the relevant information of the selected card to module G, which conveys the data to the magnetic stripe "E", all as described in detail above. Once the information is available in the magnetic stripe, smart card "A" is capable to perform as the selected card.

[0130] By another non-limiting example, modules "B", "C", "F" and "D" are fitted in a programmable device, such as cell phone or a PDA. Module G is either incorporated in the programmable device, or coupled therewith through interface. Upon user selection of card information, the information of the selected card is transmitted to the magnetic stripe "E" of card "A", via a card writer. By way of another non limiting example, smart card "A" includes also an LCD screen. When the information is sent from the said device to the magnetic stripe of the smart card, additional information (such as the name and number of the selected card) is sent to the LCD. As may be recalled instead, of magnetic stripe (E) the latter can be emulated, using, e.g., the emulation sequence described with reference to Figs. 8 to 13, above.

[0131] The present invention has been described with a certain degree of particularity, with respect to each one of its distinct aspects, but those versed in the art will readily appreciate that various alterations and modifications can be carried out, without departing from the following Claims:

IPR2025-00644 Page 01017

CLAIMS:

1. A method of writing data on magnetic stripe of a smart card by imposing magnetic field of a given polarity on each selected segment of the magnetic stripe, such that data on the magnetic stripe can be read by a magnetic card reader and interpreted as digital bits, comprising:

(i) providing a multi-dimensional conductor array placed proximate to the magnetic stripe, the number of conductors in the array is considerably smaller than the number of segments, and each segment is associated with at least two conductors;

(ii) providing current drivers for sending currents in controlled direction through the conductor array;

(iii) sending currents, using said current drivers, through conductors of the array, such that for each one of the selected segment composite currents flowing through it's associated at least two conductors overcome the coersivity of the segment of the magnetic stripe.

2. The method according to Claim 1, wherein each segment is a magnetic domain, and wherein data read from two succeeding domains corresponds to one bit.

3. The method according to Claims 1 or 2, wherein said data bits comply with the *Aiken Biphase* code.

4. The method according to anyone of the preceding Claims, wherein said array of conductors includes first array of conductors for sending currents in one direction and second array of conductors for sending currents in opposite direction.

5. The method according to anyone of the preceding Claims, wherein said multi-dimensional conductor array being a two-dimensional matrix conductor array.

6. The method according to Claim 5, wherein said two-dimensional matrix conductor array includes X conductors in the row dimension of the matrix and Y conductors in the column dimension of the matrix, such that each domain is associated with a unique entry (i,j) identified by a conductor *i* in the row dimension and conductor *j* in the column dimension of the matrix;

and wherein sending currents, using said current drivers, stipulated in (iii) includes sending a current through the *i* conductor and sending a current through the *j* conductor where the sum of the *i* current and the *j* current overcomes the coersivity of the respective domain.

IPR2025-00644 Page 01018

7. The method according to claims 5 or 6, wherein said $X=Y$ and wherein said I current and j current are of identical magnitude.

8. The method according to anyone of Claims 6 and 7, wherein said provision of two dimensional matrix includes provision of a matrix layout such that each of said X and Y conductors have a square waveform like shape and active conductor segments of each *i,j,* conductors are placed proximate and substantially parallel to their associated domain.

9. The method according to anyone of the Claims 1 to 4, wherein said multi-dimensional conductor array being a three-dimensional matrix conductor array.

10. The method according to anyone of the preceding Claims, wherein said magnetic stripe of the smart card includes four tracks.

11. The method according to Claim 10, wherein said 4 tracks magnetic stripe complies with the *American National Standards Institute (ANSI) & ISO/IEC.*

12. The method according to anyone of the preceding Claims, wherein the magnetic stripe layer is placed on top of the multi-dimensional conductor array.

13. The method according to anyone of the preceding Claims, wherein the magnetic stripe layer is placed on top of the multi-dimensional conductor array.

14. The method according to anyone of the preceding Claims, wherein said smart card being credit or debit card.

15. The method according to Claim 14, wherein said smart card serves as a multi-card credit or debit card.

16. A method for statically emulating a magnetic stripe, such that data can be read by a magnetic card reader and interpreted as digital bits, comprising:

a) providing in a smart card a conductor array proximate card's surface;

b) providing current drivers for sending currents in controlled direction through the conductor array ; and

c) sending currents, using said current drivers, through conductors of the array, for generating magnetic field of sufficient magnitude so as to be read by the magnetic card reader and interpreted as digital bits, while the card is being swiped for reading.

17. The method according to Claim 16, wherein said conductor array includes at least one conductor for each emulated magnetic domain.

IPR2025-00644 Page 01019

18. The method according to Claim 16, wherein said conductor array being multi-dimensional conductor array. The method according to Claim 16, wherein said multi-dimensional conductor array, being a two-dimensional matrix.

19. The method according to Claim 16, wherein said multi-dimensional conductor array, being a three-dimensional matrix.

20. The method according to anyone of the Claims 15 to 19, wherein said emulation being for four tracks magnetic stripe.

21. The method according to Claim 20, wherein said four tracks emulated magnetic stripe comply with the *American National Standards Institute (ANSI) & ISO/IEC.*

22. A method for dynamically emulating a magnetic stripe, such that data can be read by a magnetic card reader and interpreted as digital bits, comprising:

(i) providing at least one conductor proximate the card surface;

(ii) providing at least one current driver for sending current through the at least one conductor; and

(iii) sending variable current, using said at least one current driver, through the at least one conductor, for generating magnetic field of sufficient magnitude so as to be read by the magnetic card reader and interpreted as digital bits.

23. The method according to Claim 22, wherein said (iii) is performed whilst obviating the need to swipe the card during reading.

24. The method according to Claims 22 or 23, wherein said conductor being an elongated electronic transducer extending along major portion of the longitudinal extent of the card.

25. The method according to anyone of the Claims 22 to 24, wherein said emulation being for four tracks magnetic stripe, and wherein at least one conductor is provided for each emulated track.

26. The method according to Claim 25, wherein said four tracks emulated magnetic stripe comply with the *American National Standards Institute (ANSI) & ISO/IEC.*

27. The method according to anyone of Claims 22 to 26, wherein said variable current, changes over time in compliance with the *Aiken Biphase* code.

IPR2025-00644 Page 01020

28. The method according to anyone of Claims 22 to 27, further comprising providing magnetic coupling between the write head of a magnetic stripe writer and the at least one conductor, for entering data to the smart card.

29. A method for writing data onto a smart card, using magnetic card writer, comprising:

a) providing at least one conductor proximate the card surface ;

b) providing magnetic coupling between the write head of a magnetic stripe writer and the at least one conductor, for entering data to the smart card.

30. The method according to Claim 29, wherein said (ii) is performed whilst obviating the need to swipe the card during writing.

31. The method according to Claims 29 or 301, wherein said conductor being an elongated electronic transducer extending along major portion of the longitudinal extent of the card.

32. The method of claim 31 where the transducer is a Hall-effect device.

33. The method according to anyone of the Claims 29 to 32, wherein said data writing being for four tracks, and wherein at least one conductor is provided for each track.

34. The method according to Claim 33, wherein said four tracks comply with the *American National Standards Institute (ANSI) & ISO/IEC.*

35. The method according to anyone of Claims 29 to 34, wherein said variable current, changes over time in compliance with the *Aiken Biphase* code.

36. The method according to anyone of the Claims 16 to 21, wherein said smart card being credit or debit card.

37. The method according to Claim 36, wherein said smart card serves as a multi-card credit or debit card.

38. The method according to anyone of the Claims 22 to 28, wherein said smart card being credit or debit card.

39. The method according to Claim 38, wherein said smart card serves as a multi-card credit or debit card.

40. The method according to anyone of the Claims 29 to 35, wherein said smart card being credit or debit card.

41. The method according to Claim 40, wherein said smart card serves as a

IPR2025-00644 Page 01021

multi-card credit or debit card.

42. A method for writing data on a magnetic stripe of a magnetic card, comprising:

(i) providing a conductor array proximate to the magnetic stripe;

(ii) providing current drivers for sending currents in controlled direction through the conductor array; and

(iii) sending currents, using said current drivers, through conductors of the array, for generating magnetic field of sufficient magnitude so as to overcome the coersivity of the magnetic stripe.

43. The method according to Claim 42, wherein said conductor array includes at least one conductor for each magnetic domain in the magnetic stripe.

44. The method according to Claim 42, wherein said conductor array being multi-dimensional conductor array.

45. The method according to Claim 44, wherein said multi-dimensional conductor array, being a two-dimensional matrix.

46. The method according to Claim 44, wherein said multi-dimensional conductor array, being a three-dimensional matrix.

47. The method according to anyone of the Claims 42 to 46, wherein said writing being for four tracks magnetic stripe.

48. The method according to Claim 47, wherein said four tracks emulated magnetic stripe comply with the *American National Standards Institute (ANSI) & ISO/IEC.*

49. A system for writing data on magnetic stripe of a smart card by imposing magnetic field of a given polarity on each selected segment of the magnetic stripe, such that data on the magnetic stripe can be read by a magnetic card reader and interpreted as digital bits, comprising:

a multi-dimensional conductor array placed proximate to the magnetic stripe, the number of conductors in the array is considerably smaller than the number of segments, and each segment is associated with at least two conductors;

current drivers for sending currents in controlled direction through the conductor array;

a device for sending currents, using said current drivers, through conductors

of the array, such that for each one of the selected segment composite currents flowing through it's associated at least two conductors overcome the coersivity of the segment of the magnetic stripe.

50. A system for statically emulating a magnetic stripe, such that data can be read by a magnetic card reader and interpreted as digital bits, comprising:

a conductor array, fitted in a smart card proximate the card's surface;

current drivers for sending currents in controlled direction through the conductor array;

a device for sending currents, using said current drivers, through conductors of the array, for generating magnetic field of sufficient magnitude so as to be read by the magnetic card reader and interpreted as digital bits, while the card is being swiped for reading.

51. A system for dynamically emulating a magnetic stripe, such that data can be read by a magnetic card reader and interpreted as digital bits, comprising:

at least one conductor placed proximate the card surface;

at least one current driver for sending current through the at least one conductor;

a device for sending variable current, using said at least one current driver, through the at least one conductor, for generating magnetic field of sufficient magnitude so as to be read by the magnetic card reader and interpreted as digital bits.

52. A system for writing data onto a smart card, using magnetic card writer, comprising:

at least one conductor placed proximate the card surface;

means for providing magnetic coupling between the write head of a magnetic stripe writer and the at least one conductor, for entering data to the smart card.

53. A system for writing data on a magnetic stripe of a card, comprising:

a conductor array capable of being placed proximate to the magnetic stripe;

current drivers configured to send currents in controlled direction through the conductor array;

a device configured to sending currents, using said current drivers, through conductors of the array, for generating magnetic field of sufficient magnitude so as to overcome the coersivity of the magnetic stripe.

54. A system for writing data on a magnetic stripe of a card, comprising:

a writing device capable of writing data onto the magnetic stripe being placed in proximity thereto; the writing device is characterized in having no moving parts.

55. The system according to Claim 49, wherein said device includes a programmable device and associated input means and storage for storing information indicative of plurality of cards and, in response to user selection, data is converted to currents sent in controlled direction through the conductor array.

56. The system according to Claim 55, wherein said programmable device, associated input means and storage form part of the card.

57. The system according to Claim 55, wherein said programmable device, associated input means and storage, or parts thereof are accommodated in external device communicating with the card.

58. The system according to Claim 57, wherein said external device being a PDA or cellular telephone.

59. The system according to anyone of Claims 55 to 58, wherein said data being at least one member selected from the group that includes: data indicative of a selected card, data required to activate a card, data required to configure a new card, data required to complete transaction.

60. The system according to Claim 50, wherein said device includes a programmable device and associated input means and storage for storing information indicative of plurality of cards and in response to user selection data is converted to currents sent through the conductor array.

61. The system according to Claim 60, wherein said programmable device, associated input means and storage form part of the card.

62. The system according to Claim 60, wherein said programmable device, associated input means and storage, or parts thereof are accommodated in external device communicating with the card.

63. The system according to Claim 62, wherein said external device being a PDA or cellular telephone.

64. The system according to anyone of Claims 60 to 63, wherein said data being at least one member selected from the group that includes: data indicative of a selected card, data required to activate a card, data required to configure a new card, data

required to complete transaction.

65. The system according to Claim 51, wherein said device includes a programmable device and associated input means and storage for storing information indicative of plurality of cards and in response to user selection data is converted to variable current sent to the at least one conductor.

66. The system according to Claim 65, wherein said programmable device, associated input means and storage form part of the card.

67. The system according to Claim 65, wherein said programmable device, associated input means and storage, or parts thereof are accommodated in external device communicating with the card.

68. The system according to Claim 67, wherein said external device being a PDA or cellular telephone.

69. The system according to anyone of Claims 65 to 68, wherein said data being at least one member selected from the group that includes: data indicative of a selected card, data required to activate a card, data required to configure a new card, data required to complete transaction.

70. A smart card storing information of multiple cards; said card includes processor and associated device capable of conveying data indicative of a selected card from among said plurality of cards, to a magnetic stripe of the smart card, so as to be read by a magnetic card reader.

71. A smart card storing information of multiple cards; said card includes processor and associated device capable of emulating data indicative of a selected card from among said plurality of cards; said emulated data are capable of being read by a magnetic card reader.

72. A system of storing data indicative of multiple cards in a storage area of a programmable module; the system is capable of transferring data to a magnetic stripe of a card.

73. The system according to Claim 72, wherein said programmable module is fitted in external device capable of communicating with the card.

74. The system according to Claim 73, wherein said external device being PDA or cellular phone.

75. The system according to Claim 53, wherein said system includes a

programmable device and associated input means and storage for storing information indicative of plurality of cards and, in response to user selection, data is converted to currents sent in controlled direction through the conductor array.

76. The system according to Claim 75, wherein said programmable device, associated input means and storage, conductor array and current drivers are all integral in the system.

77. The system according to Claim 75, wherein said programmable device, associated input means and storage, or parts thereof are accommodated in external device that is coupled to said conductor array and current drivers.

78. The system according to Claim 77, wherein said external device being a PDA or cellular telephone.

79. The system according to Claim 76, wherein said system is included in PDA or cellular telephone.

80. The system according to anyone of Claims 75 to 79, wherein said data being at least one member selected from the group that includes: data indicative of a selected card, data required to activate a card, data required to configure a new card, data required to complete transaction.

81. The system according to Claim 54, wherein said system includes a programmable device and associated input means and storage for storing information indicative of plurality of cards and, in response to user selection, data is converted to currents sent in controlled direction through the conductor array.

82. The system according to Claim 81, wherein said programmable device, associated input means and storage, conductor array and current drivers are all integral in the system.

83. The system according to Claim 81, wherein said programmable device, associated input means and storage, or parts thereof are accommodated in external device that is coupled to said conductor array and current drivers.

84. The system according to Claim 83, wherein said external device being a PDA or cellular telephone.

85. The system according to Claim 82, wherein said system is included in PDA or cellular telephone.

86. The system according to anyone of Claims 81 to 87, wherein said data

being at least one member selected from the group that includes: data indicative of a selected card, data required to activate a card, data required to configure a new card, data required to complete transaction.

IPR2025-00644 Page 01027

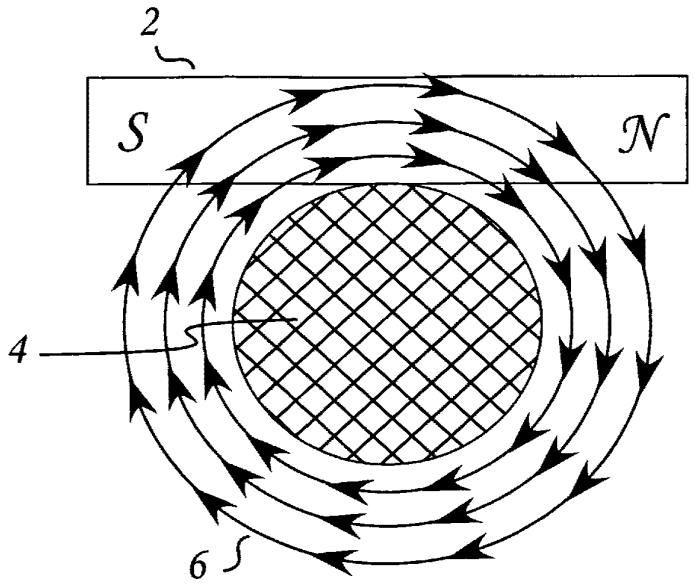


Fig. 1

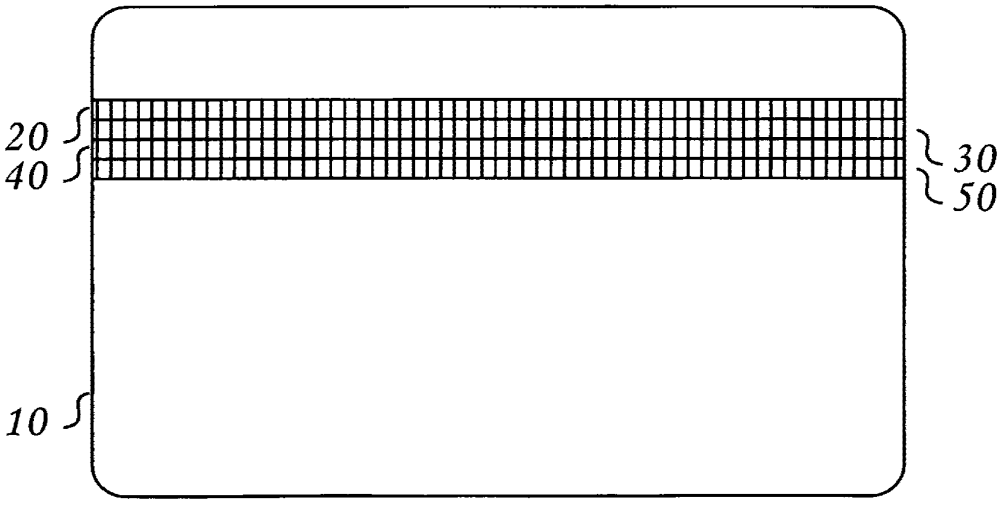


Fig. 2

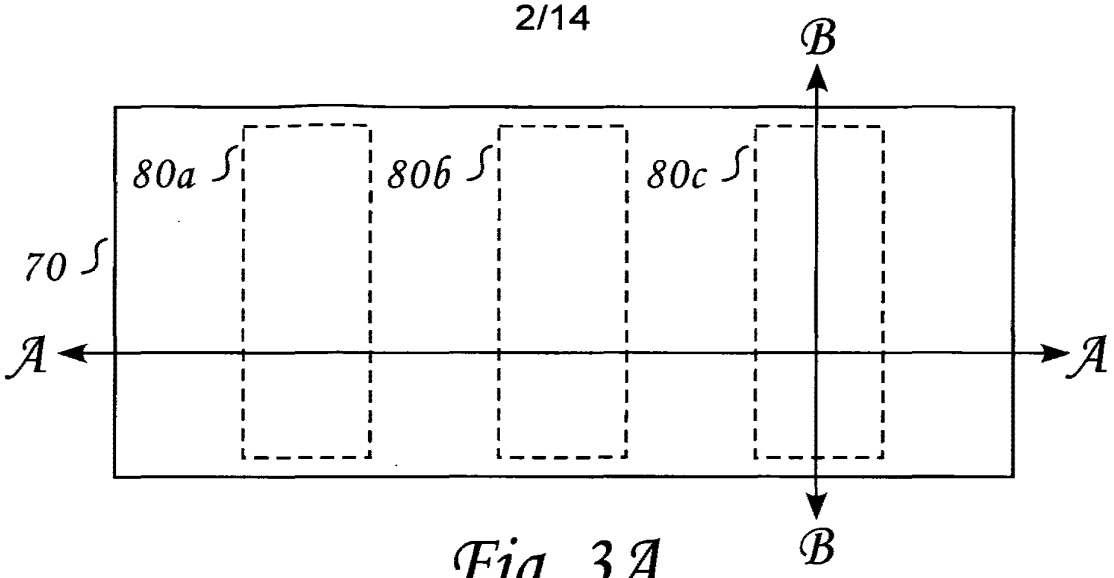


Fig. 3A

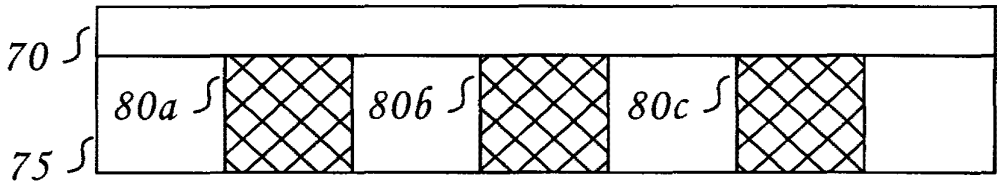


Fig. 3B

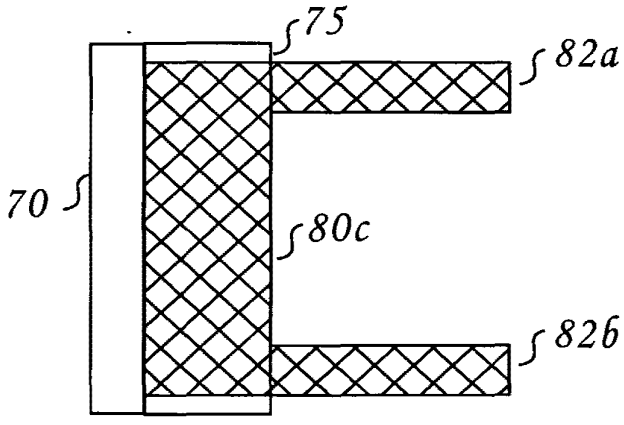


Fig. 3C

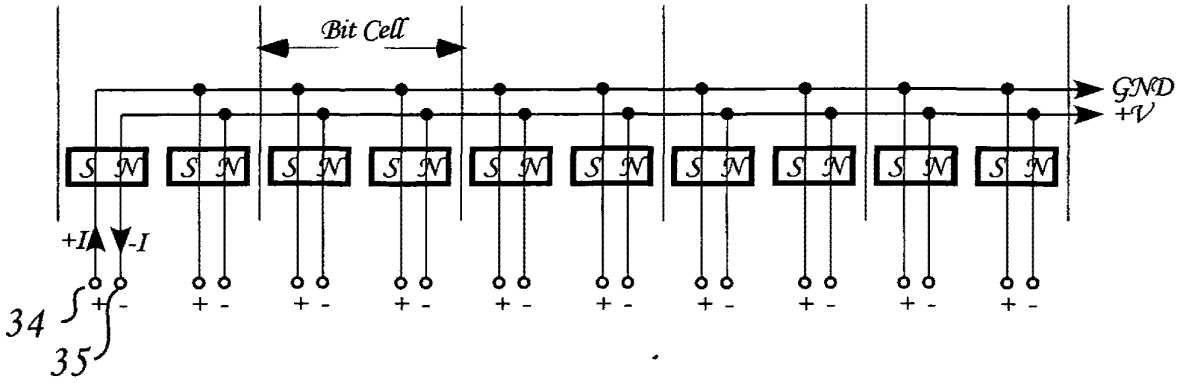


Fig. 3D

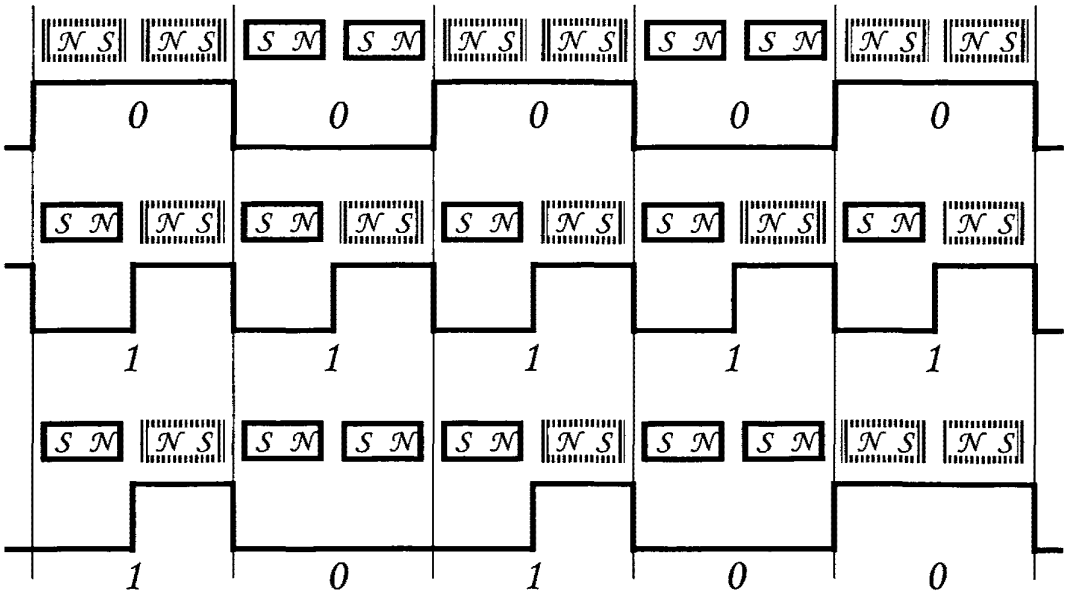


Fig. 3E

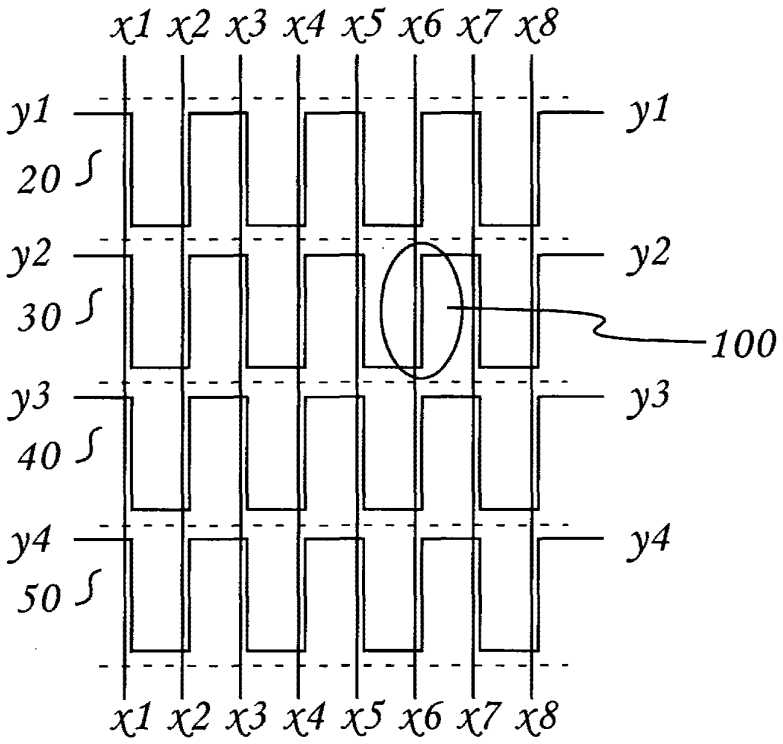

x1 x2 x3 x4 x5 x6 x7 x8
y1
20
y2
30
y3
40
y4
50
y1
y2
100
y3
y4
x1 x2 x3 x4 x5 x6 x7 x8

Fig. 4A

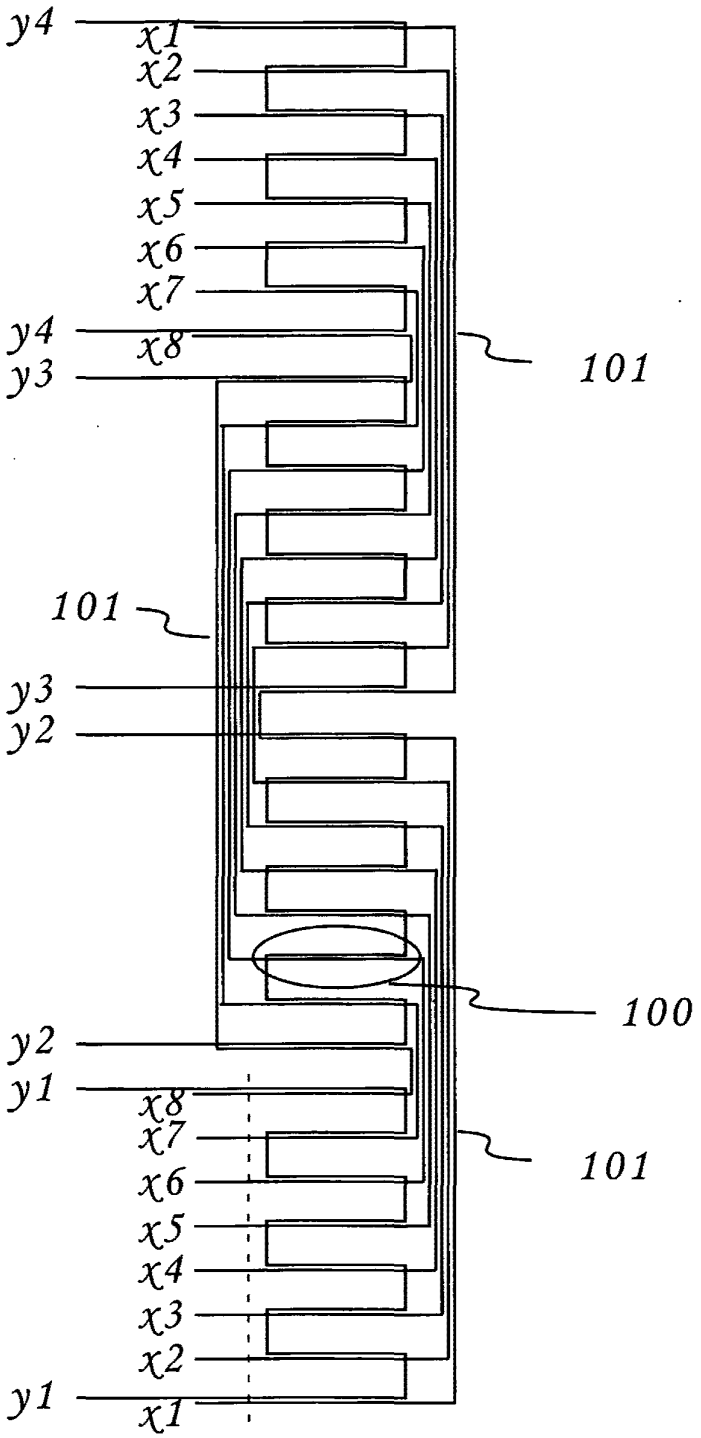

y4
x1
x2
x3
x4
x5
x6
x7
y4
x8
y3
101
101
y3
y2
100
y2
y1
x8
x7
x6
x5
x4
x3
x2
y1
x1
101

Fig. 4B

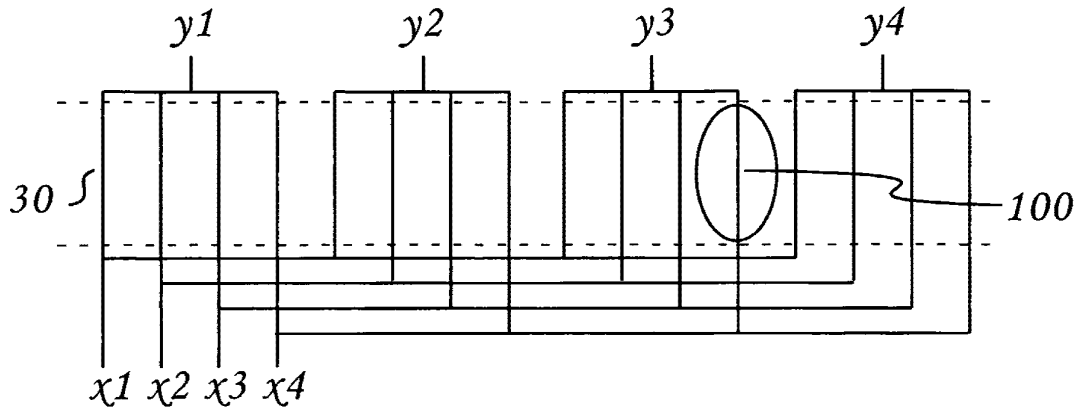

y1
y2
y3
y4
30
100
x1
x2
x3
x4

Fig. 4C

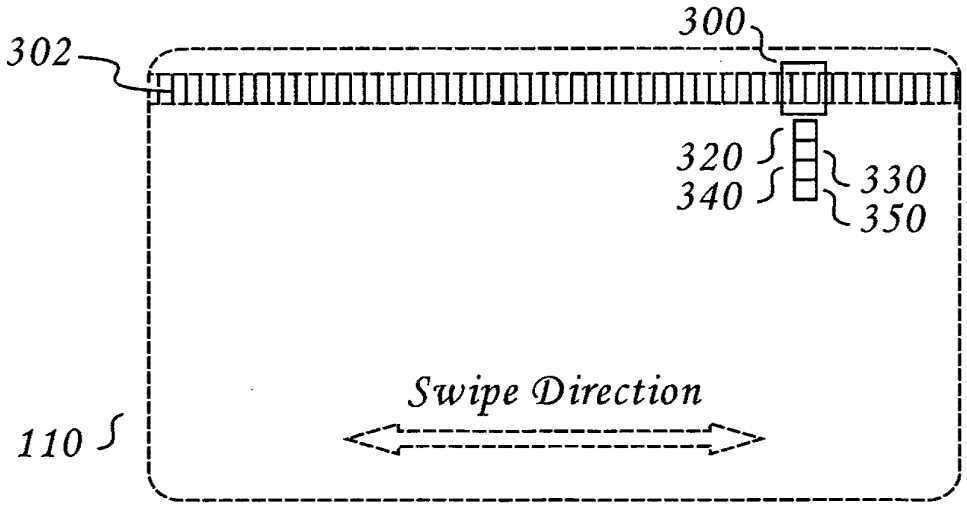

300
302
320
340
330
350
Swipe Direction
110

Fig. 4D

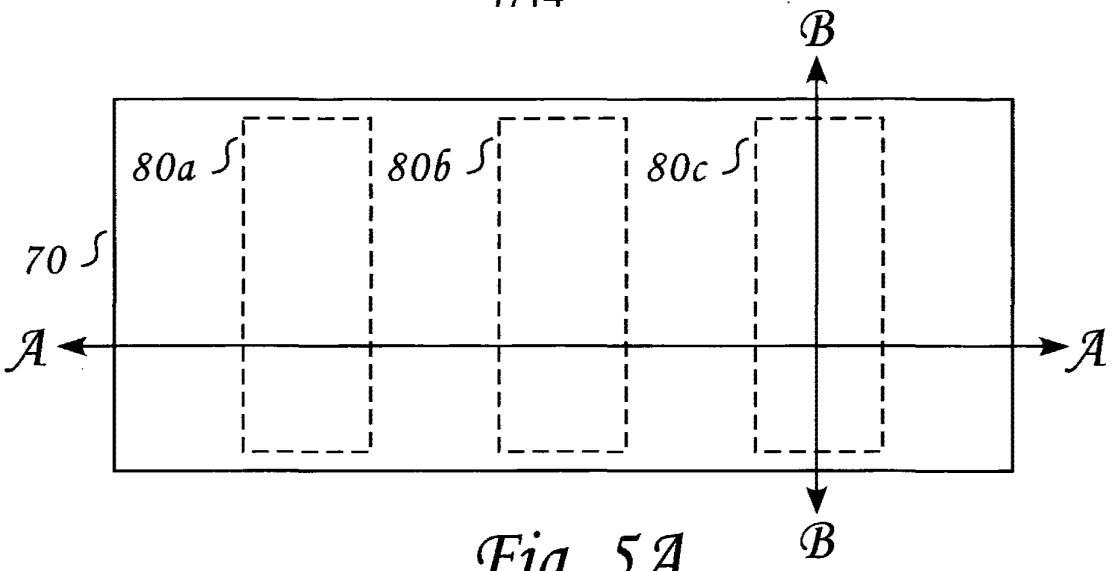


Fig. 5A

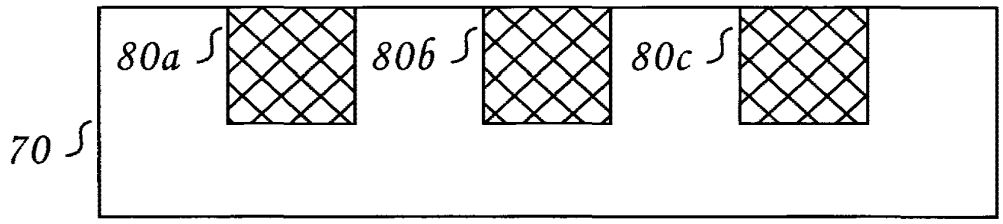


Fig. 5B

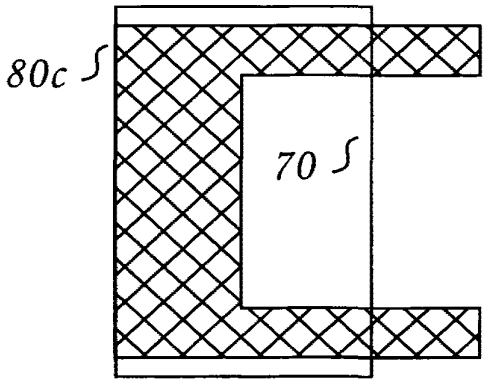


Fig. 5C

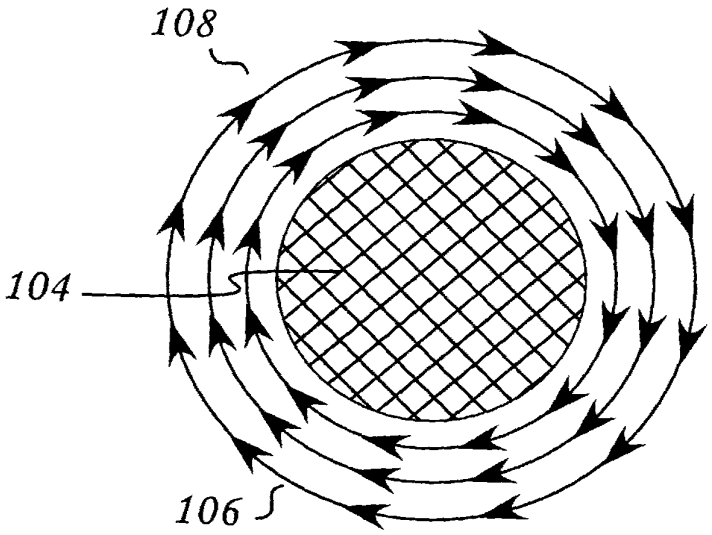


Fig. 6

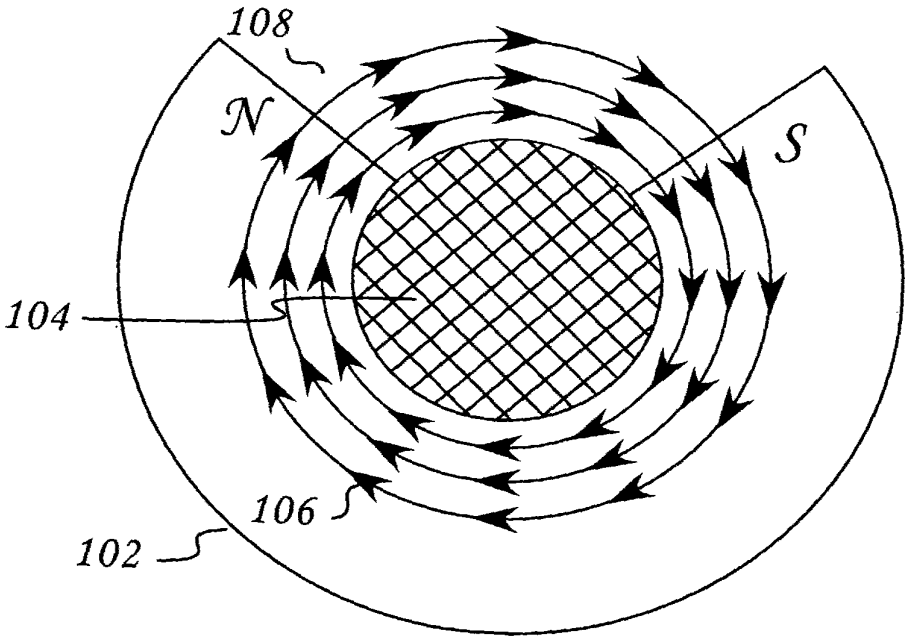


Fig. 7

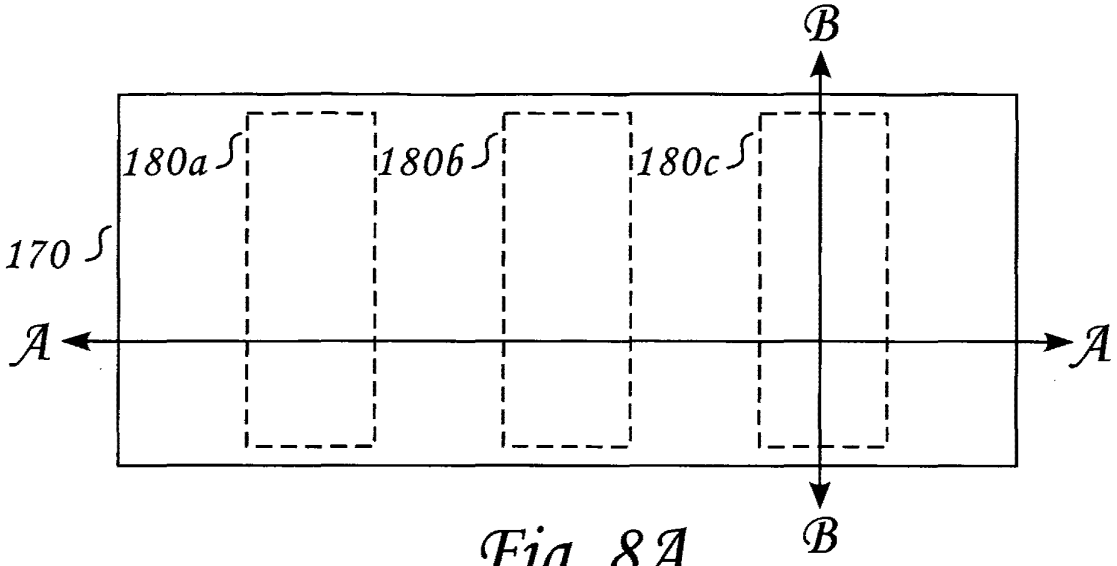


Fig. 8A

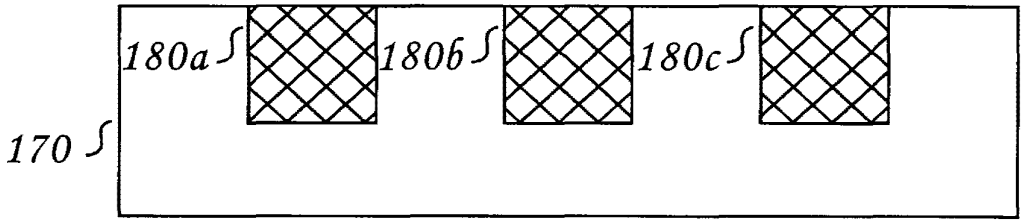


Fig. 8B

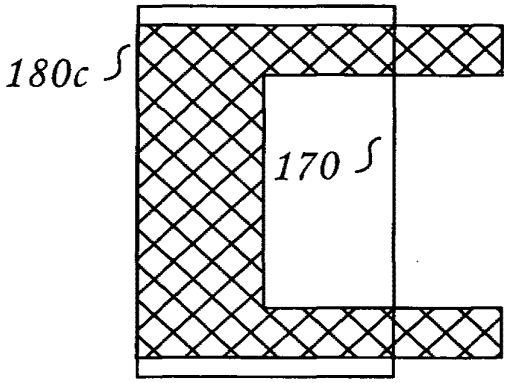


Fig. 8C

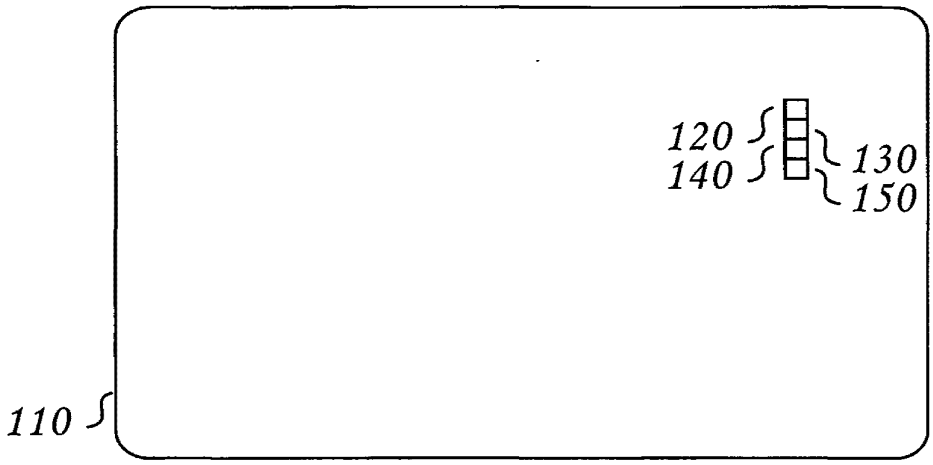


Fig. 9

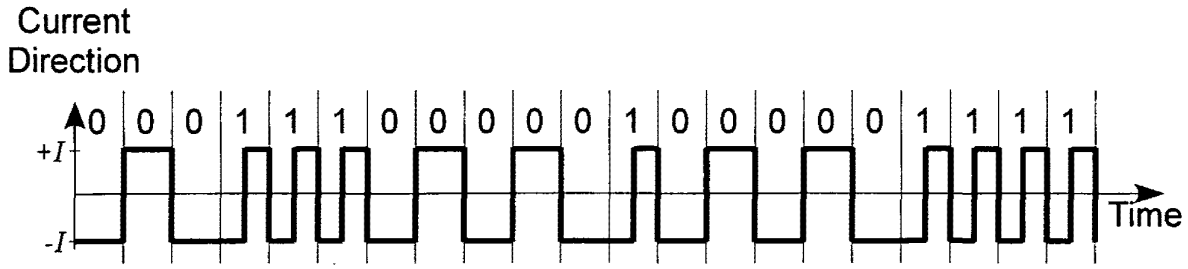


Fig. 10

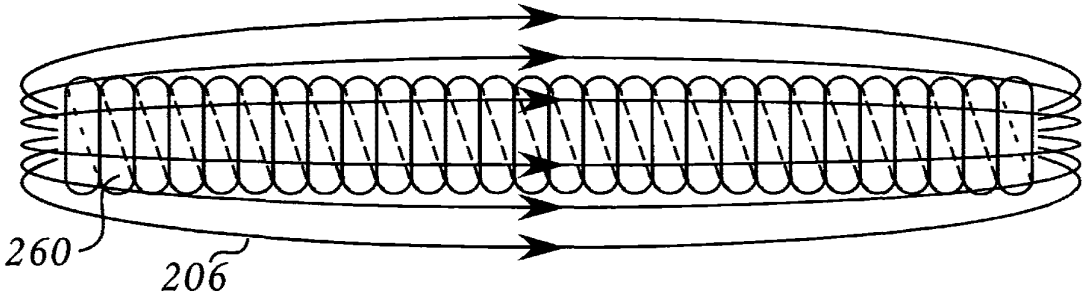


Fig. 11

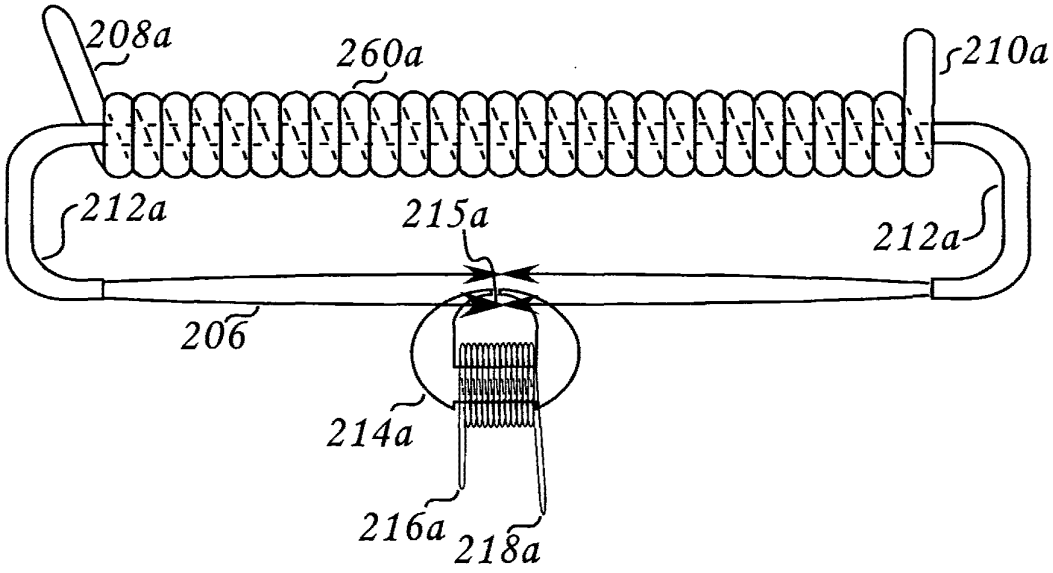

208a
260a
210a
212a
215a
212a
206
214a
216a
218a

Fig. 12

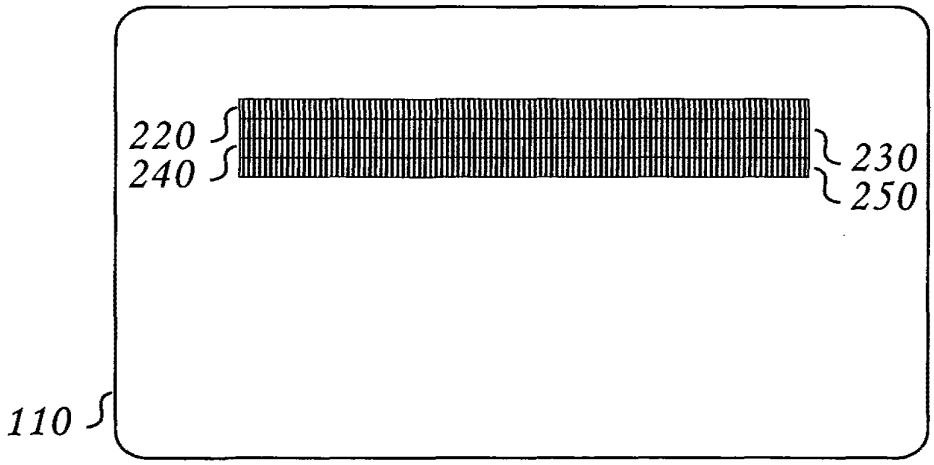

220
240
230
250
110

Fig. 13

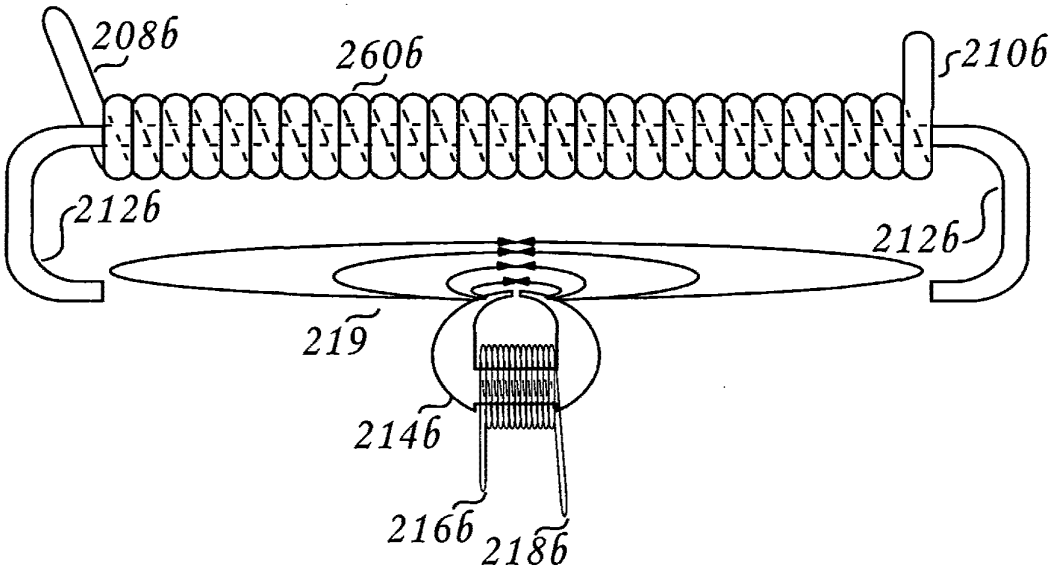


Fig. 14

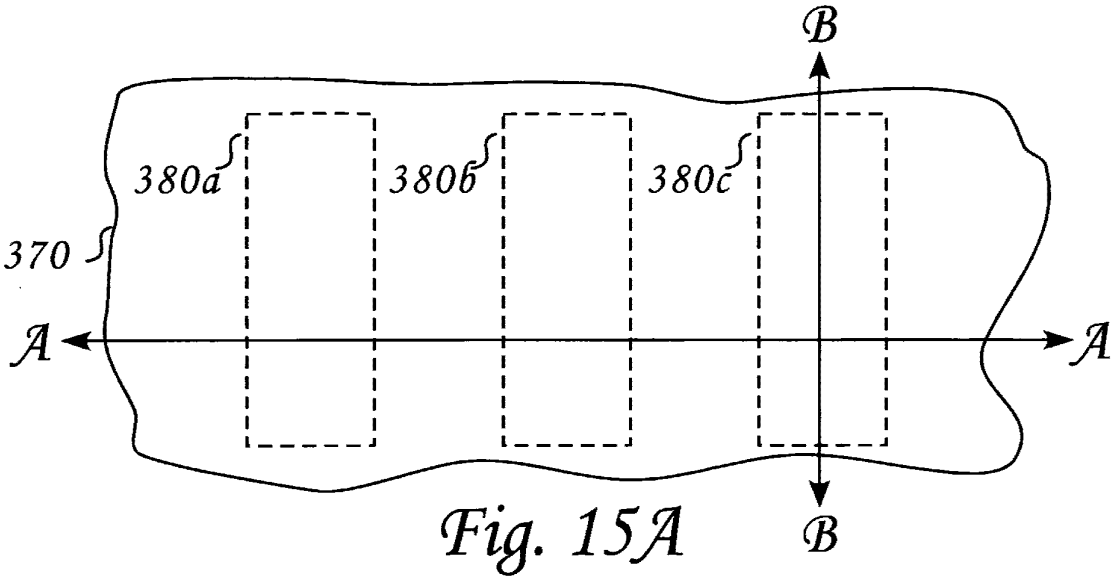


Fig. 15A

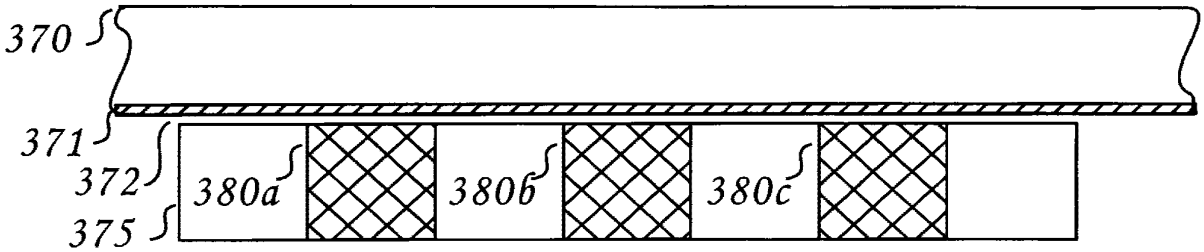


Fig. 15B

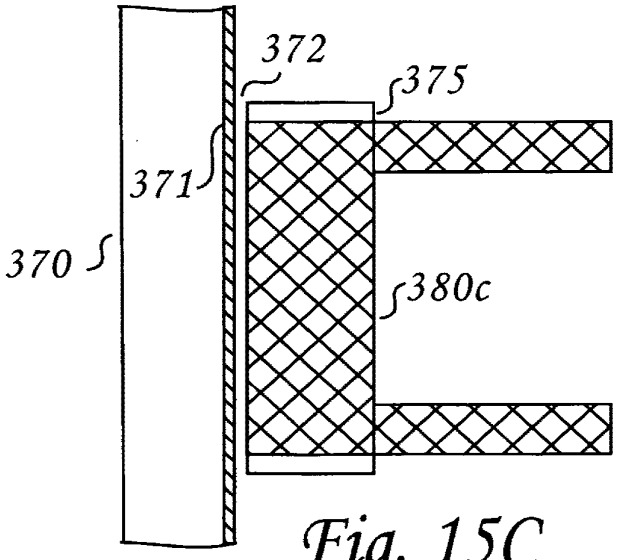


Fig. 15C

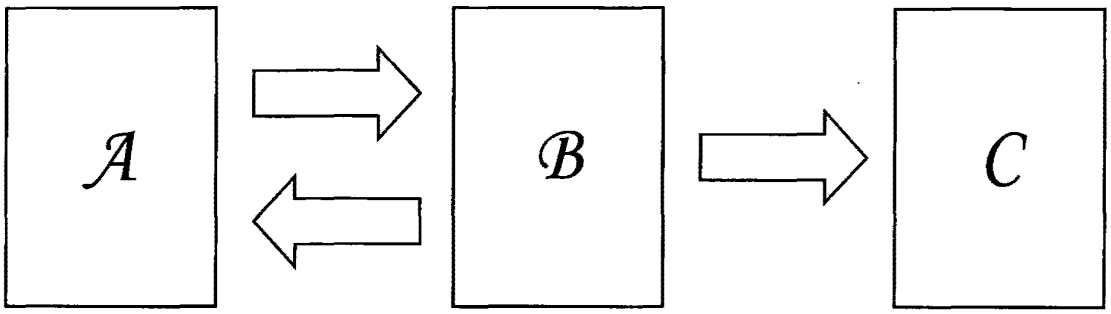


Fig. 16

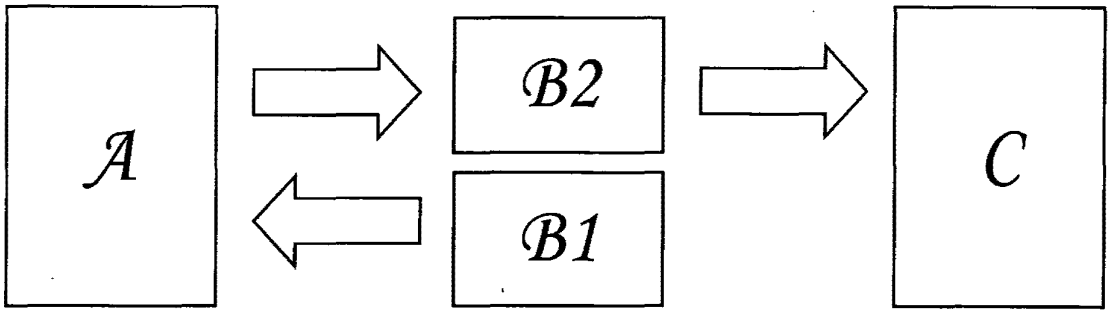


Fig. 16A

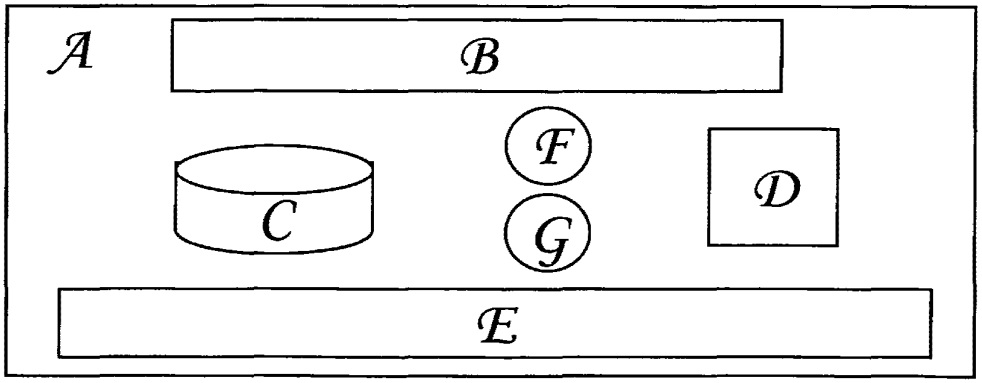


Fig. 17

(12)特許協力条約に基づいて公開された国際出願

(19) 世界知的所有権機関
国際事務局

(43) 国際公開日
2005 年3 月24 日 (24.03.2005)

PCT

(10) 国際公開番号
WO 2005/027030 A1

(51) 国際特許分類[7]: G06K 19/00, G06T 7/00, B42D 15/10

(21) 国際出願番号: PCT/JP2004/013473

(22) 国際出願日: 2004 年9 月9 日 (09.09.2004)

(25) 国際出願の言語: 日本語

(26) 国際公開の言語: 日本語

(30) 優先権データ:
特願2003-317580 2003 年9 月9 日 (09.09.2003) JP
特願 2003-426322
2003 年12 月24 日 (24.12.2003) JP
特願2004-163800 2004 年6 月1 日 (01.06.2004) JP

(71) 出願人 (米国を除く全ての指定国について): 株式会社ヒューマンテクノロジーズ (HUMAN TECHNOLOGIES, INC.) [JP/JP]; 〒213-0001 神奈川県 川崎市 高津区溝の口２－１１－８ Kanagawa (JP).

(72) 発明者; および

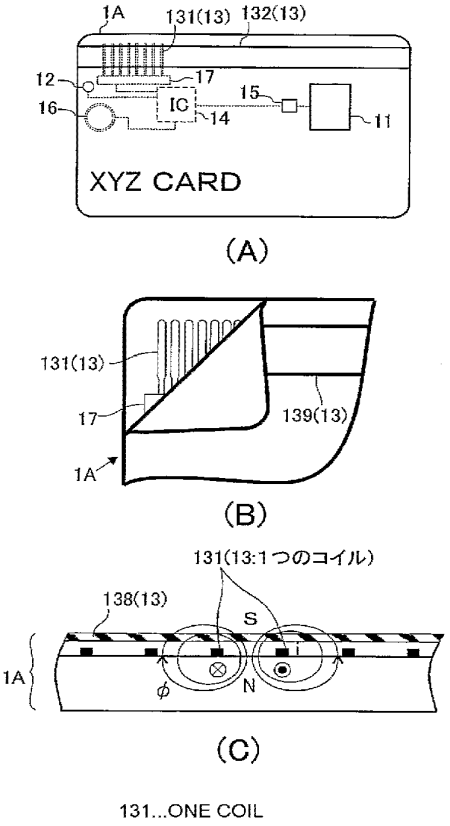
(75) 発明者/出願人 (米国についてのみ): 黒川 不二雄 (KUROKAWA,Fujio) [JP/JP]; 〒852-8013 長崎県 長崎市 梁川町１９番地１－２０２号 Nagasaki (JP). 樋口 剛 (HIGUCHI,Tsuyoshi) [JP/JP]; 〒852-8045 長崎県 長崎市 錦３丁目１５－１４ Nagasaki (JP). 阿部 晋一 (ABE,Shinichi) [JP/JP]; 〒335-0014 埼玉県 戸田市 喜沢南１－４－１７－１０１９ Saitama (JP). 地蔵 秀秋 (JIZO,Hideaki) [JP/JP]; 〒142-0064 東京都 品川区 旗の台３－１５－１ Tokyo (JP). 藤村 美智 (FUJIMURA,Michi) [JP/JP]; 〒213-0033 神奈川県 川崎市 高津区下作延３７９ Kanagawa (JP). 荒井 博雄 (ARAI,Hiroo) [JP/JP]; 〒246-0013 神奈川県 横浜市 瀬谷区相沢２－２９－１－Ｂ１０１ Kanagawa (JP).

(74) 代理人: 平石 利子 (HIRAISHI,Toshiko); 〒105-0003 東京都 港区 西新橋１丁目１８番１５号 Tokyo (JP).

/続葉有/

(54) Title: MAGNETIC STRIPE GENERATING DEVICE, AUTHENTICATION DEVICE, AUTHENTICATION SYSTEM AND MAGNETIC STRIPE GENERATING METHOD

(54) 発明の名称: 磁気ストライプ生成装置、認証装置、認証システムおよび磁気ストライプ生成方法



(57) Abstract: A magnetic stripe generating device capable of generating, by a current, all or part of magnetic flux generating elements constituting a magnetic stripe, a magnetic stripe generating method, and an authentication device capable of generating a correct magnetic stripe pattern in a magnetic stripe only when finger-print matching is successful and an authentication system. A magnetic strip generating device which forms all or part of magnetic flux generating elements of a magnetic stripe by magnetic fluxes generated by a plurality of coils or conductors, characterized in that provided are the above coils or conductors and a drive circuit for supplying respective currents of specified magnitudes to relative coils or conductors.

(57) 要約: 本発明は、磁気ストライプを構成する磁束発生要素の全部または一部を電流により生成することができる磁気ストライプ生成装置、磁気ストライプ生成方法、および、指紋照合が成功したときにのみ磁気ストライプに正しい磁気ストライプパターンを生成できる認証装置、認証システムを提供する。複数のコイルまたは導線が生成する磁束により磁気ストライプの磁束発生要素の一部または全部が形成される磁気ストライプ生成装置であって、前記コイルまたは前記導線と、前記コイルまたは前記導線に当該コイルまたは当該導線ごとに、所定の大きさの電流を流す駆動回路とを備えたことを特徴とする。

WO 2005/027030 A1

(81) 指定国 (表示のない限り、全ての種類の国内保護が可能): 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, 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, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) 指定国 (表示のない限り、全ての種類の広域保護が可能): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), ユーラシア (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), ヨーロッパ (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).

規則4.17に規定する申立て:
— *US*のみのための発明者である旨の申立て (規則 *4.17(iv)*)

添付公開書類:
— 国際調査報告書

２文字コード及び他の略語については、定期発行される各*PCT*ガゼットの巻頭に掲載されている「コードと略語のガイダンスノート」を参照。

明　細　書

磁気ストライプ生成装置、認証装置、認証システムおよび磁気ストライプ生成方法

技術分野

本発明は、磁気ストライプを構成する磁束発生要素の全部または一部を電流により生成することができる磁気ストライプ生成装置、磁気ストライプ生成方法、および、指紋照合が成功したときにのみ磁気ストライプに正しい磁気ストライプパターンを生成できる認証装置、認証システムに関する。

背景技術

一般的なキャッシュカード（銀行カード）、クレジットカードでは、裏面にテープ状の磁気記録領域が形成され、当該磁気記録領域に、磁気ストライプの形態でシリアル番号等が記録されている。

たとえばキャッシュカード所有者は、当該キャッシュカードを銀行等に備えたキャッシング装置（磁気読み取り装置）にセットして、当該装置に設けられたキーボード等から暗証番号を入力する。

この暗証番号と、磁気ストライプに予め記録されている暗証番号との照合がキャッシング装置により行なわれ、照合が成功すれば利用者はキャッシング等を行なうことができる。

また、たとえばクレジットカード所有者が当該クレジットカードを用いて店舗にて商品を購入するときには、当該店舗の店員は、ク

レジットカードをカードリーダにセットし、オンラインでその有効性をチェックする。クレジットカードが有効であれば、利用者は所定の用紙に署名をし、この署名とカードに記載された署名との同一性が認められれば商品購入が可能となる。

また、ホテルのルームキーとして使用されるカードキーでは、表面または裏面の磁気記録領域に所定のコードが記録されている。ドアに設置された施錠装置にはカードリーダが設けられており、利用者は開錠に際してカードリーダにカードキーを差し込み、磁気記録領域に記録されたコードが施錠装置に設定されているコードと符合したときにのみ開錠がなされる。

発明の開示

ところが、上記したキャッシュカード、クレジットカード、カードキーでは、磁気記録領域に記録された情報を解析することが可能であり、カードが盗まれた場合には、不正利用者による使用がなされる危険性がある。

また、キャッシュカードやクレジットカードでは、所有者本人の顔写真を表面に表示したカードも多く使われるようになっている。しかし、カード自体が偽造されるときには顔写真も不正利用を行なう者の顔写真に置き換えられるので、偽造キャッシュカードによるキャッシング、偽造クレジットカードによる高額商品の購入、あるいは偽造カードキーによる不法な入室が可能となってしまう。

本発明の目的は、磁気ストライプを構成する磁束発生要素の全部または一部を電流により生成することができる磁気ストライプ生

成装置および磁気ストライプ生成方法を提供することである。

本発明の他の目的は、指紋照合が成功したときにのみ磁気ストライプに正しい磁気ストライプパターンを生成できる認証装置および認証システムを提供することである。

本発明は、（１）複数のコイルまたは導線が生成する磁束により磁気ストライプの磁束発生要素の一部または全部が形成される磁気ストライプ生成装置であって、前記コイルまたは前記導線と、前記コイルまたは前記導線に当該コイルまたは当該導線ごとに、所定の大きさの電流を流す駆動回路と、を備えたことを特徴とする磁気ストライプ生成装置を要旨とする。

本発明は、（２）前記コイルまたは前記導線が形成されている領域は、着磁されていないことを特徴とする（１）に記載の磁気ストライプ生成装置を要旨とする。

本発明は、（３）前記コイルまたは前記導線の少なくとも１つが発生する磁束が、すでに着磁により形成された磁束発生要素が生成している磁束をキャンセルし、または当該磁束発生要素の磁気極性を反転させることを特徴とする（１）に記載の磁気ストライプ生成装置を要旨とする。

本発明は、（４）前記駆動回路は、一時的に所定の磁極ストライプパターンを形成することを特徴とする（１）から（３）の何れかに記載の磁気ストライプ生成装置を要旨とする。

本発明は、（５）前記コイルまたは前記導線に磁気ストライプ読出しヘッドの読み取りギャップ位置検出用の微小電流を流し、当該

電流値の変化を検出する位置検出回路を備えた磁気ストライプ生成装置であって、

前記駆動回路は、前記位置検出回路が前記コイルまたは前記導線が前記ギャップに位置したことを検出したときは、前記コイルまたは前記導線に前記所定の大きさの電流を流すことを特徴とする（１）から（４）の何れかに記載の磁気ストライプ生成装置を要旨とする。

本発明は、（６）（１）から（５）の何れかに記載の磁気ストライプ生成装置を備えた認証装置であって、少なくとも１つの指紋情報を登録指紋情報として保存する指紋情報保存手段と、指紋検出手段と、前記指紋検出手段からの検出情報を受け取って検出指紋情報を生成する検出指紋情報生成手段と、前記検出指紋情報と前記登録指紋情報との一致を検出する指紋一致検出手段（ＣＰＵとＲＯＭまたはＲＡＭ内プログラムがこの手段として機能することができる）とを備えた認証装置であって、前記駆動回路は、前記指紋一致検出手段が、前記検出指紋情報と前記登録指紋情報との一致を検出したときは、所定の磁極ストライプパターンを生成する前記所定の大きさの電流を前記コイルまたは前記導線に流すことを特徴とする認証装置を要旨とする。

本発明は、（７）クレジットカードまたはキャッシュカードとして使用されることを特徴とする（６）に記載の認証装置を要旨とする。

本発明は、（８）施錠または開錠のためのキーとして使用されることを特徴とする（６）に記載の指紋照合機能付き認証装置を要旨

とする。

本発明は、（９）（６）から（９）の何れかに記載の認証装置と、磁気ストライプ読出しヘッドを備えたことを特徴とする。

本発明は、（１０）認証装置と磁気信号受信装置を備えた認証システムであって、前記認証装置は、少なくとも１つの指紋情報を登録指紋情報として保存する指紋情報保存手段と、指紋検出手段と、前記指紋検出手段からの検出情報を受け取って検出指紋情報を生成する検出指紋情報生成手段と、前記検出指紋情報と前記登録指紋情報との一致を検出する指紋一致検出手段と、前記指紋一致検出手段が、前記検出指紋情報と前記登録指紋情報との一致を検出判断したときに周波数変調されていない磁気信号を前記磁気信号受信装置に出力する磁気信号発生手段と、を備えたことを特徴とする認証システムを要旨とする。

本発明は、（１１）複数のコイルまたは導線が生成する磁束により磁気ストライプの磁束発生要素の一部または全部を形成する磁気ストライプ生成方法であって、

前記コイルまたは前記導線に当該コイルまたは当該導線ごとに、所定の大きさの電流を流す駆動ステップとを有することを特徴とする磁気ストライプ生成方法を要旨とする。

本発明は、（１２）前記コイルまたは前記導線が形成されている領域は、着磁されていないことを特徴とする（１１）に記載の磁気ストライプ生成方法を要旨とする。

本発明は、（１３）前記コイルまたは前記導線の少なくとも１つが発生する磁束が、すでに着磁形成されている磁束発生要素が生成

している磁束をキャンセルし、または当該磁束発生要素の磁気極性を反転させることを特徴とする（１１）または（１２）に記載の磁気ストライプ生成方法を要旨とする。

本発明は、（１４）前記駆動ステップにおいては、一時的に所定の磁極ストライプパターンを形成することを特徴とする（１１）から（１３）の何れかに記載の磁気ストライプ生成方法を要旨とする。

本発明は、（１５）前記コイルまたは前記導線に磁気ストライプ読出しヘッドの読み取りギャップ位置検出用の微小電流を流し、当該電流値の変化を検出するギャップ位置検出ステップを備えた磁気ストライプ生成方法であって、前記駆動ステップでは、前記ギャップ位置検出ステップにおいて前記コイルまたは前記導線が前記ギャップに位置したことが検出されたときは、前記コイルまたは前記導線に前記所定の大きさの電流を流すことを特徴とする（１１）から（１４）の何れかに記載の磁気ストライプ生成方法を要旨とする。

本発明は、（１６）（１１）から（１５）の何れかに記載の磁気ストライプ生成方法におけるステップを含む認証方法であって、少なくとも１つの指紋情報を登録指紋情報として保存する指紋情報保存手段と、指紋検出ステップと、前記指紋検出ステップからの検出情報を受け取って検出指紋情報を生成する検出指紋情報生成ステップと、前記検出指紋情報と前記登録指紋情報との一致を検出する指紋一致検出ステップ（ＲＯＭまたはＲＡＭ内プログラムがこの手段として機能することができる）とを備えた認証方法であって、前記駆動ステップでは、前記指紋一致検出ステップにより、前記検出

指紋情報と前記登録指紋情報との一致が検出されたときは、所定の磁極ストライプパターンを生成する前記電流を前記コイルまたは前記導線に流すことを特徴とする認証方法を要旨とする。

本発明は、（１７）クレジットカードまたはキャッシュカードとして使用することを特徴とする（１６）に記載の認証方法を要旨とする。

本発明は、（１８）施錠または開錠のためのキーとして使用することを特徴とする（１５）に記載の認証方法を要旨とする。

図面の簡単な説明

図１：本発明の指紋照合機能付きカードの一例を示す外観図である。

図２：（Ａ）は磁気ストライプを搭載したカードの回路構成を示す図、（Ｂ）はカードの内部にコイルが設けられている様子を示す図、（Ｃ）はコイルに電流が流れ磁気ストライプが形成された様子（磁束が発生する様子）を示す図である。

図３：（Ａ）はコイルの空間配置モデルであり、（Ｂ）はコイルが生成する磁束を示す図である。

図４：（Ａ）は導線の空間配置モデルであり、（Ｂ）は導線が生成する磁束を示す図である。

図５：（Ａ），（Ｂ）は、グランドとして導体面を使用した例を示す図である。

図６：（Ａ）は溝Ｇを形成した合成樹脂基板を示す図、（Ｂ）は溝に無電界メッキを施すことでコイルを形成する様子を示す図で

ある。

図７：（Ａ）は指紋処理用ＩＣの具体例を示す図であり、（Ｂ）はＲＯＭ内情報を示す図である。

図８：カードの動作を示すフローチャートである。

図９：（Ａ）は磁気ヘッドが導線を流れる電流を検出するときの様子を示す図、（Ｂ）は導線の背面に磁性体を配置した例を示す図である。

図１０：（Ａ），（Ｂ）は、位置検出回路を備えた他のカードの説明図である。

図１１：（Ａ）は無線送信器を搭載したカードの回路構成を示す図、（Ｂ）は指紋処理用ＩＣの内部構成を示す図である。

図１２：指紋登録用ホルダにカードがセットされている様子を示す説明図である。

図１３：指紋登録の処理を示すフローチャートである。

発明を実施するための最良の形態

図１は本発明の認証装置をクレジットカードやキャッシュカード（以下、単に「カード」と言う）を例を示す外観図である。カード１の表面には、図１に示すように、指紋センサ１１と、発光ダイオード１２と、磁気ストライプ１３が形成されている。なお、指紋センサ１１、発光ダイオード１２および磁気ストライプ１３は、図示しないエンボス部を避けて形成されている。

図２（Ａ）の回路構成図に示すように、カード（図２（Ａ）では符号１Ａで示す）の磁気ストライプ１３部分には、磁性体膜１３９

が形成されている。本実施形態のカード１Ａでは、磁気ストライプ１３を構成する磁束発生要素の一部が、複数のコイル１３１により形成され、残りの磁束発生要素が着磁により形成されている。この回路は、上記した指紋センサ１１、発光ダイオード１２、磁気ストライプ１３のほか、指紋処理用ＩＣ１４と、起動スイッチ１５と、バッテリー１６と、駆動回路１７とを備えている。

指紋センサ１１（本発明の「指紋情報検出手段」として機能する）は、カード１Ａに搭載できるものであればどのようなタイプのもの（光学式センサ、感圧式センサ、指紋の微細な凹凸を静電気により検出する静電気検出式センサ）でも使用できる。また、指紋センサ１１は、指を滑らすライン式のものであってもよいし、指を押し当てるエリア式のものであってもよい。

ＬＥＤ１２は、本実施形態では、たとえば指紋照合が成功したときに点灯して、利用者にその旨を知らせたり、電池が消耗したときに点滅する等のために使用されるが、本発明においては必須ではない。

磁気ストライプ１３は、図２（Ｂ）に示すようにコイル（磁束発生要素）１３１を備えている。このコイル１３１はカード１Ａの厚み部分に埋設されている。

指紋処理用ＩＣ１４は、指紋センサ１１からの検出信号を受け取り、指紋照合処理を行なうプロセッサである。指紋処理用ＩＣ１４に代えて、複数の回路装置（ＣＰＵおよびメモリ）を用いることもできる。

起動スイッチ１５は、起動するときにオンするスイッチである。

バッテリー１６は、起動スイッチ１５がオンすることにより、指紋センサ１１、ＬＥＤ１２、指紋処理用ＩＣ１４および駆動回路１７に電力を供給する。なお、図２（Ａ）では電源回路の図示は省略してある。

本実施形態ではバッテリー１６によりカード１Ａに電力を供給しているが、カード１Ａに電源入力端子を設けておき、外部電源（たとえば、磁気ストライプ読み取り装置に備えた電源）から電力の供給を受けるようにしてもよい。

駆動回路１７は、コイル１３１に所定値の電流を流す（ここでは、電流を流さない場合は値０の電流を流すものと定義する）ことができる。図２（Ｃ）に示すようにコイル１３１に電流ｉが流れると、磁気ストライプ１３の所定領域（コイル１３１が設けられた領域）には、磁束φが形成される。コイル１３１には、もともと電流が流れることがないダミーコイルを含めることができる。

なお、本実施形態では、磁気ストライプの着磁されていない領域にコイル１３１を設けたが、着磁されている領域にコイル１３１を設け、このコイルによる磁束により当該着磁領域の磁束をキャンセルするようにしてもよい。図２ではコイル１３１が設けられている領域に磁性体膜を存在したが、この磁生体膜を形成しないようにもできる。本実施形態では、磁気ストライプ１３の磁束発生要素の一部をコイル１３１により形成したが（すなわち、着磁により形成される通常の磁束発生要素とコイル１３１により生成される磁束発生要素との組み合わせにより形成したが）、磁束発生要素の全部をコイル１３１により形成するようにしてもよい。

図３（Ａ），（Ｂ）は、磁気ストライプ１３の磁束発生要素の一部を複数のコイルにより形成したカード１Ｂの説明図であり、（Ａ）はコイル１３２の空間配置モデルであり、（Ｂ）はコイル１３２が生成する磁束を示す図である。図２のカード１Ａでは、コイル１３１のコイル面はカード面に平行であったが、本実施形態のカード１Ｂでは、コイル１３２のコイル面はカード面に垂直としてある。

図４（Ａ），（Ｂ）は、磁気ストライプ１３の磁束発生要素の一部が複数の導線により形成されたカード１Ｃの説明図であり、（Ａ）は導線１３３の空間配置モデルであり、（Ｂ）は導線１３３が生成する磁束を示す図である。導線１３３は、グランド１３５に接続されている。図４（Ａ），（Ｂ）では、グランド１３５は一本の導線としてあるが、この導線の代わりに図５（Ａ），（Ｂ）に示すよう導体面を使用することもできる。

カード１Ａのコイル１３１、カード１Ｂのコイル１３２、カード１Ｃの導線１３３、グランド１３５は、たとえば周知の合成樹脂メッキ技術によりプラスチック基板上に作成することができる。

指紋センサ１１、発光ダイオード１２、磁気ストライプ１３、指紋処理用ＩＣ１４、起動スイッチ１５、バッテリー１６、駆動回路１７間を接続する回路は、これら素子を搭載するための端子やこれらを搭載するための端子等は、合成樹脂メッキ技術により作成することができる。

たとえば、図４（Ａ）に示した導線１３３は、図６（Ａ）に示すように、溝Ｇを形成した合成樹脂基板Ｂの溝Ｇ部分に、図６（Ｂ）に示したように、無電界メッキを施すことで（さらに、電界メッキ

を施すことで）形成することができる。

図７（Ａ）に示すように、指紋処理用ＩＣ１４は、ＣＰＵ１４１と、ＲＯＭ１４２と、ＲＡＭ１４３と、ＬＥＤ１２用のスイッチ（ＳＷ）１４４と、タイマー１４５と、指紋センサ１１用インタフェース１４６１，起動スイッチ１５用インタフェース１４６２とからなる。

ＣＰＵ１４１は、ＲＯＭ１４２内のシステムプログラムと協働して、カード１（１Ａ，１Ｂ，１Ｃ）の全体を制御する。ＲＯＭ１４２には、図７（Ｂ）に示すように、システムプログラム、指紋センサ１１用のドライバ（ソフトウェア）、駆動回路１７用のドライバ、検出指紋情報生成プログラム、指紋一致検出プログラム等のソフトウェアのほか、選択コイル情報等のデータが格納されている。さらに、ＲＯＭ１４２の指紋情報保存領域は本発明の「指紋情報保存手段」として機能し登録指紋情報等が登録される他、指紋情報以外のデータも格納されている。

ＲＡＭ１４３は、ＣＰＵ１４１の作業領域等として使用される。ＬＥＤ１２用のスイッチ（ＳＷ）１４４はＣＰＵ１４１からの制御信号によりオン・オフ動作するトランジスタスイッチである。タイマー１４５は、カード１（１Ａ，１Ｂ，１Ｃ）が有効となる時間を計数する。指紋センサ１１用のインタフェース１４６１，起動スイッチ１５用インタフェース１４６２はゲート回路により構成される。

以下、図８のフローチャートにより、カード１の動作を説明する。

利用者が起動スイッチ１５をオンすると、カード１のシステムが

オンとなり（ｓｔａｒｔ）、指紋処理用ＩＣ１４が指紋センサ１１用のドライバを駆動し、指紋センサ１１により指紋検出が行なわれる（Ｓ１０１）。指紋処理用ＩＣ１４は、検出データをインタフェース１４６１を介して受け取り、受信データをコード化する（Ｓ１０２）。

このコード化したデータを、ＲＯＭ１４２に記憶されている指紋情報（登録指紋コード）と照合する（Ｓ１０３）。指紋処理用ＩＣ１４は、ＲＯＭ１４２に一致しているコードがないとき（Ｓ１０４の「ＮＯ」）はカード電源をオフし処理を終了する（ｅｎｄ）が、一致しているコードがあるときは（Ｓ１０４の「ＹＥＳ」：すなわち、照合が成功したとき）は、ＬＥＤ１２を点灯する（Ｓ１０５）とともに、駆動回路１７に選択データを出力する（Ｓ１０６）。駆動回路１７は所定のコイルまたは導線に電流を流当該コイルまたは導線から磁束を発生する（あるいはコイルまたは導線に相当する部分のもともと磁化されている領域の磁束をキャンセルする）。

本実施形態では、ＬＥＤ１２が点灯している間は、カード１の機能が有効となる。ＬＥＤ１２点灯後、所定期間が経過したときは（Ｓ１０７）、ＬＥＤ１２を消灯し（Ｓ１０８）カード電源をオフし処理を終了する（ｅｎｄ）。

図９（Ａ）は、磁気ヘッド２１が、導線１３３を流れる電流を検出するときの様子を示している。図９（Ａ）では、１ｍｍに１０本のコイルが形成されている。また、図９（Ｂ）は、導線１３３の背面に磁性体を配置した例を示している。なお、図示はしないが、導線１３３の周囲を絶縁性磁性体により形成することができる。

図１０（Ａ），（Ｂ）は、位置検出回路を備えたカードの説明図である。図１０（Ａ）の回路構成図に示すように、本実施形態のカード（符号１Ｄで示す）は基本的にはカード１Ｃと同じである。本実施形態では、指紋処理用回路は、制御用ＩＣ１４１と指紋照合処理回路１４２と位置検出回路１４３とからなる。

本実施形態では、位置検出回路１４３は導線１３４に微小電流を流しており、位置検出回路１４３は導線１３４が磁気ヘッドのギャップに位置したことを、微小電流の値の変換により検出できる。制御用ＩＣ１４１は、導線１３４が磁気ヘッドのギャップに位置したときに、駆動回路１７のキャパシタＣに蓄積されたに充電された電荷を、抵抗Ｒを介して導線１３４に流すことができる。図１０（Ｂ）は、図１０（Ａ）の起動スイッチ１５に代えて、キーを用いた例を示している。ここではキーは、「０」，「１」の２種のキー１８１，１８２からなり、たとえば、０１０１の順でキーが押されたときにのみキー制御回路１８０が、バッテリー１６からの電力を電源回路１６１に送出する。

図１１（Ａ）は、指紋照合機能付きカードを示す他の実施形態を示す図である。

指紋照合機能付きカード４Ａは、指紋センサ４１、発光ダイオード４２、アンテナ４３と、指紋処理用ＩＣ４４と、起動スイッチ４５と、バッテリー４６と、駆動回路４７とを有している。

図１１（Ｂ）に示すように指紋処理用ＩＣ４４は、ＣＰＵ４４１と、ＲＯＭ４４２と、ＲＡＭ４４３と、ＬＥＤ４２用のスイッチ（ＳＷ）４４４と、タイマー４４５と、指紋センサ４１用のインタフェ

ース４４６１，起動スイッチ４５用のインタフェース４４６２と、磁気信号発生回路４４７とからなる。

ＲＯＭ４４２には図４（Ｂ）に示したプログラムが内蔵されている。指紋処理用ＩＣ４４を構成するＲＯＭ４４２（本発明の「指紋情報保存手段」としても機能する）を有しており、ＲＯＭ４４２は、少なくとも１つの指紋情報を登録指紋情報として保存する。

指紋センサ４１は、指紋を検出する。指紋処理用ＩＣ４４を構成するＲＯＭ４４２の検出指紋情報生成プログラム（本発明の「検出指紋情報生成手段」として機能する）は、指紋センサ４１からの検出情報を受け取って検出指紋情報を生成する。

ＲＯＭ４４２の指紋一致検出手段は、検出指紋情報が登録指紋情報に一致するか一致しないかを判断する。磁気信号発生回路４４７（本発明の「磁気信号発生手段」として機能する）は、周波数変調されていない磁気信号（たとえば、強さ、極性がタイミングで異なる信号）を出力することができる。

磁気信号発生回路４４７は、ＲＯＭ４４２に格納された指紋検証プログラム（指紋情報一致判断手段）が、検出指紋情報が登録指紋情報に一致すると判断したときに、図示しないカードリーダに認証成功情報を出力する。

本発明では、一枚のカード１を複数の利用者が利用するために、複数の指紋を当該カードに登録することができる。

図１２には、指紋登録用ホルダ９にカード１がセットされている様子が示されている。この指紋登録用ホルダ９にカードがセットされると、指紋の登録が可能となる。指紋登録用ホルダ９には、登録

モードであることを示すＬＥＤ９１と、指紋登録が完了したことを示す登録確認ＬＥＤ９２が設けられている。

図１３は、指紋登録の処理を示すフローチャートである。カード１が、指紋登録用ホルダ９にセットされると、当該カードに指紋登録モードとする信号が指紋登録用ホルダ９に設けられた図示しないアンテナ，端子から送信される。指紋登録モードでは、新たなユーザの指紋を追加するようにできる。

図１３では、カード１が、指紋登録用ホルダ９にセットされると電源がオンし登録モードになりＬＥＤ９１が点灯する（Ｓ２０１）。ユーザが指を指紋センサ１１に押し当てると（Ｓ２０２）起動スイッチが動作し指紋検出が行なわれる（Ｓ２０３）。検出データはコード化され（Ｓ２０４）、当該コードは一時保存される（Ｓ２０５）。ユーザが一旦指を指紋センサ１１から離し、再度押し当てたことを起動スイッチが検知すると（Ｓ２０６）、指紋検出（Ｓ２０７）、コード化（Ｓ２０８）、コードの一時保存（Ｓ２０９）がなされる。このコードと、前回の指紋検出によりより得られたコードとを比較し（Ｓ２１０）、一致していれば、これを指紋コードとして登録し（Ｓ２１１）、登録確認ＬＥＤ９２を点灯し処理を終了し、一致していなければ処理をステップＳ２０２に戻す。

以上の実施形態では、カード１にバッテリー１６を搭載した例を説明した。この場合、バッテリー１６を充電できるようにカード１を構成することができるし、バッテリー１６とともにまたはバッテリー１６に代えてキャパシタを搭載することもできる。もちろんカード１にはバッテリーを充電するための端子を設けることもでき

るし、マイクロ波等により充電する場合には充電用のアンテナやコイルを設けることもできる。さらに、カード１にはバッテリー１６を搭載せずに、所定の電源供給端子から電力の供給を受けるように構成してもよい。

産業上の利用可能性

本発明の磁気ストライプ生成装置および磁気ストライプ生成方法によれば、磁気ストライプを構成する磁束発生要素の全部または一部を電流により生成することができる。

また、認証装置および認証システムによれば、指紋照合が成功したときにのみ磁気ストライプに正しい磁気ストライプパターンを生成できる。特に、本発明の認証装置は、キャッシュカード、クレジットカード、カードキー等に搭載できるので、既存のカード読み取り装置にそのまま適用することも可能である。この場合、指紋照合が成功したときにのみカードの機能が有効となり、したがって、カード紛失等に伴うカードの不正使用、偽造されたカードによる不正使用を防止できる。

本発明の認証装置をたとえばキャッシュカード、クレジットカード、カードキーに搭載する場合、複数の磁気ストライプパターンを、ＲＯＭ等の記憶装置に記憶させておき、カードに備えたキーボード等により、複数の磁気ストライプパターンのうちの１つを選択して、当該パターンを磁気ストライプ生成装置により生成するようにしてもよい。

また、本発明の認証装置をたとえばキャッシュカード、クレジッ

トカード、カードキーに搭載する場合、磁気発生要素（認証が成功したときに生成される磁気ストライプパターン）を、既存の磁気ストライプカードの磁束発生要素（着磁された磁気ストライプパターン）として構成することができる。

また、本発明の認証装置および認証システムは、カードに限らず、貯金通常、保険証、パスポート等の通常の磁気ストライプが使用される対象に適用することができる。

請　求　の　範　囲

1．　複数のコイルまたは導線が生成する磁束により磁気ストライプの磁束発生要素の一部または全部が形成される磁気ストライプ生成装置であって、

前記コイルまたは前記導線と、

前記コイルまたは前記導線に当該コイルまたは当該導線ごとに、所定の大きさの電流を流す駆動回路と、

を備えたことを特徴とする磁気ストライプ生成装置。

2．　前記コイルまたは前記導線が形成されている領域は、着磁されていないことを特徴とする請求項1に記載の磁気ストライプ生成装置。

3．　前記コイルまたは前記導線の少なくとも1つが発生する磁束が、すでに着磁により形成された磁束発生要素が生成している磁束をキャンセルし、または当該磁束発生要素の磁気極性を反転させることを特徴とする請求項1に記載の磁気ストライプ生成装置。

4．　前記駆動回路は、一時的に所定の磁極ストライプパターンを形成することを特徴とする請求項1から3の何れかに記載の磁気ストライプ生成装置。

5．　前記コイルまたは前記導線に磁気ストライプ読出しヘッドの読み取りギャップ位置検出用の微小電流を流し、当該電流値の変化を検出する位置検出回路を備えた磁気ストライプ生成装置であって、

前記駆動回路は、前記位置検出回路が前記コイルまたは前記導線

が前記ギャップに位置したことを検出したときは、前記コイルまたは前記導線に前記所定の大きさの電流を流すことを特徴とする請求項１から４の何れかに記載の磁気ストライプ生成装置。

６．　請求項１から５の何れかに記載の磁気ストライプ生成装置を備えた認証装置であって、

少なくとも１つの指紋情報を登録指紋情報として保存する指紋情報保存手段と、

指紋検出手段と、

前記指紋検出手段からの検出情報を受け取って検出指紋情報を生成する検出指紋情報生成手段と、

前記検出指紋情報と前記登録指紋情報との一致を検出する指紋一致検出手段と、

を備えた認証装置であって、

前記駆動回路は、前記指紋一致検出手段が、前記検出指紋情報と前記登録指紋情報との一致を検出したときは、所定の磁極ストライプパターンを生成する前記所定の大きさの電流を前記コイルまたは前記導線に流す、

ことを特徴とする認証装置。

７．　クレジットカードまたはキャッシュカードとして使用されることを特徴とする請求項６に記載の認証装置。

８．　施錠または開錠のためのキーとして使用されることを特徴とする請求項６に記載の指紋照合機能付き認証装置。

９．　請求項６から８の何れかに記載の認証装置と、磁気ストライプ読出しヘッドを備えたことを特徴とする認証システム。

１０．　認証装置と磁気信号受信装置を備えた認証システムであって、

前記認証装置は、

少なくとも１つの指紋情報を登録指紋情報として保存する指紋情報保存手段と、

指紋検出手段と、

前記指紋検出手段からの検出情報を受け取って検出指紋情報を生成する検出指紋情報生成手段と、

前記検出指紋情報と前記登録指紋情報との一致を検出する指紋一致検出手段と、

前記指紋一致検出手段が、前記検出指紋情報と前記登録指紋情報との一致を検出判断したときに周波数変調されていない磁気信号を前記磁気信号受信装置に出力する磁気信号発生手段と、

を備えたことを特徴とする認証システム。

１１．　複数のコイルまたは導線が生成する磁束により磁気ストライプの磁束発生要素の一部または全部を形成する磁気ストライプ生成方法であって、

前記コイルまたは前記導線に当該コイルまたは当該導線ごとに、所定の大きさの電流を流す駆動ステップと、

を有することを特徴とする磁気ストライプ生成方法。

１２．　前記コイルまたは前記導線が形成されている領域は、着磁されていないことを特徴とする請求項１１に記載の磁気ストライプ生成方法。

１３．　前記コイルまたは前記導線の少なくとも１つが発生する磁

束が、すでに着磁形成されている磁束発生要素が生成している磁束をキャンセルし、または当該磁束発生要素の磁気極性を反転させることを特徴とする請求項１１または１２に記載の磁気ストライプ生成方法。

１４．　前記駆動ステップにおいては、一時的に所定の磁極ストライプパターンを形成することを特徴とする請求項１１から１３の何れかに記載の磁気ストライプ生成方法。

１５．　前記コイルまたは前記導線に磁気ストライプ読出しヘッドの読み取りギャップ位置検出用の微小電流を流し、当該電流値の変化を検出するギャップ位置検出ステップを備えた磁気ストライプ生成方法であって、

前記駆動ステップでは、前記ギャップ位置検出ステップにおいて前記コイルまたは前記導線が前記ギャップに位置したことが検出されたときは、前記コイルまたは前記導線に前記所定の大きさの電流を流すことを特徴とする請求項１１から１４の何れかに記載の磁気ストライプ生成方法。

１６．　請求項１１から１５の何れかに記載の磁気ストライプ生成方法におけるステップを含む認証方法であって、

少なくとも１つの指紋情報を登録指紋情報として保存する指紋情報保存手段と、

指紋検出ステップと、

前記指紋検出ステップからの検出情報を受け取って検出指紋情報を生成する検出指紋情報生成ステップと、

前記検出指紋情報と前記登録指紋情報との一致を検出する指紋

一致検出ステップと、

を備えた認証方法であって、

前記駆動ステップでは、前記指紋一致検出ステップにより、前記検出指紋情報と前記登録指紋情報との一致が検出されたときは、所定の磁極ストライプパターンを生成する前記電流を前記コイルまたは前記導線に流す、

ことを特徴とする認証方法。

１７．　クレジットカードまたはキャッシュカードとして使用することを特徴とする請求項１６に記載の認証方法。

１８．　施錠または開錠のためのキーとして使用することを特徴とする請求項１５に記載の認証方法。

図1

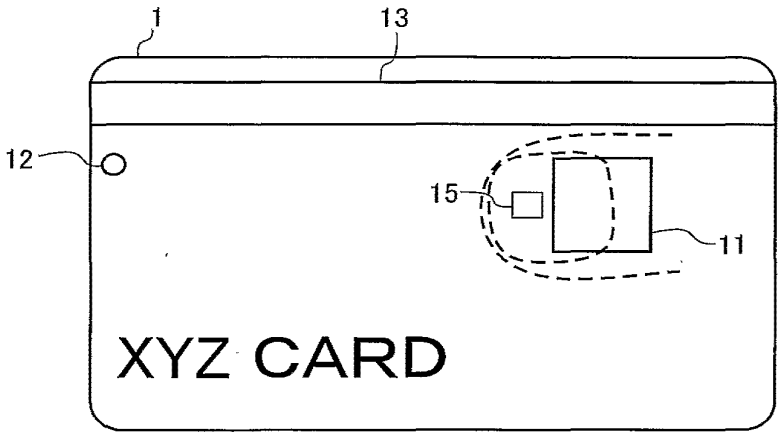
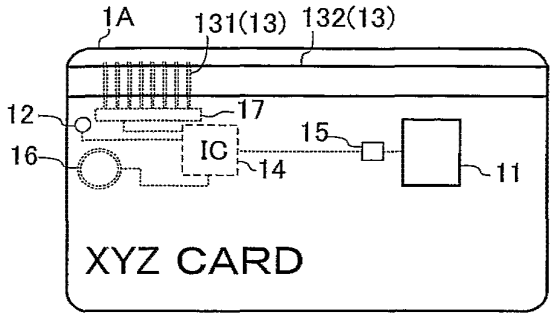
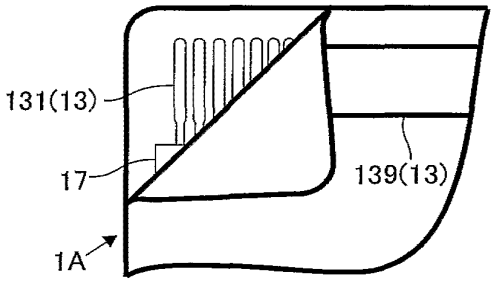


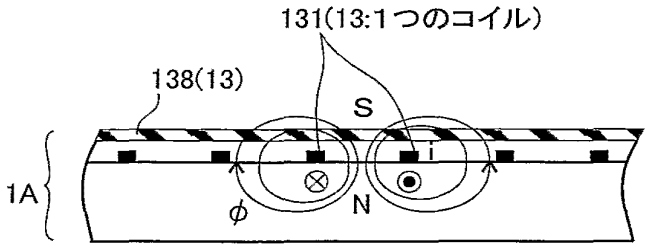
図2


1A
131(13)
132(13)
12
17
15
16
IC
14
11
XYZ CARD

(A)

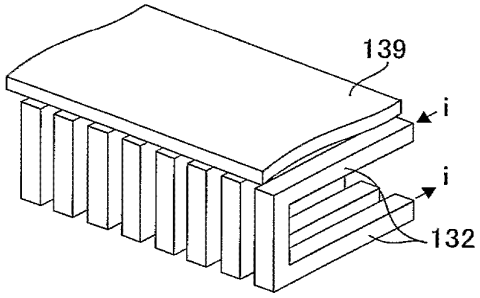

131(13)
17
139(13)
1A

(B)

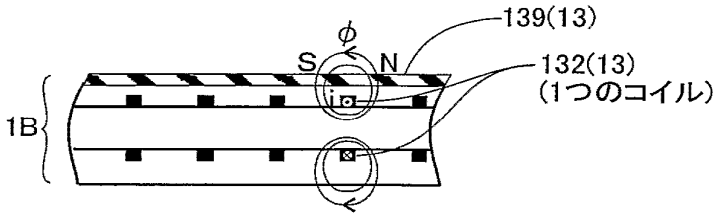

131(13:1つのコイル)
138(13)
S
1A
ϕ
N

(C)

図3

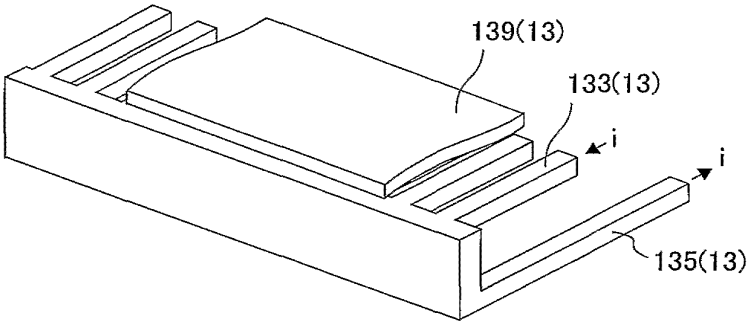


(A)

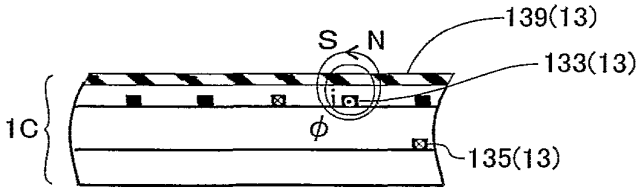


(B)

図4

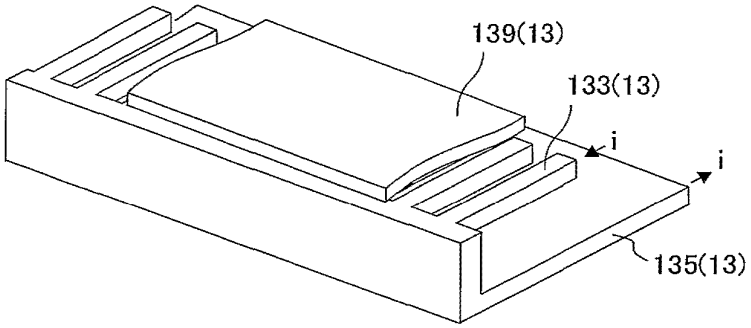


(A)

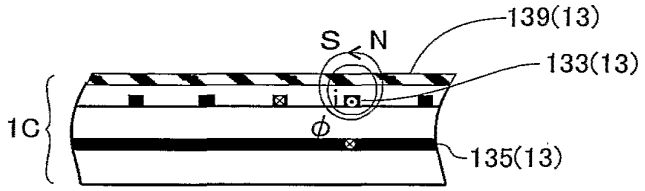


(B)

図5

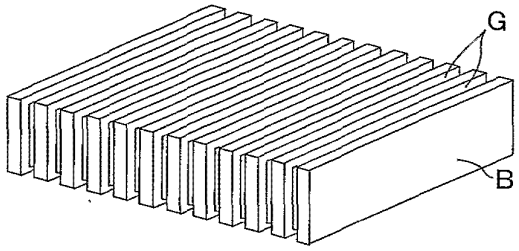


(A)

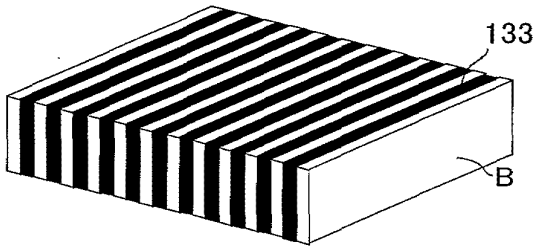


(B)

図6

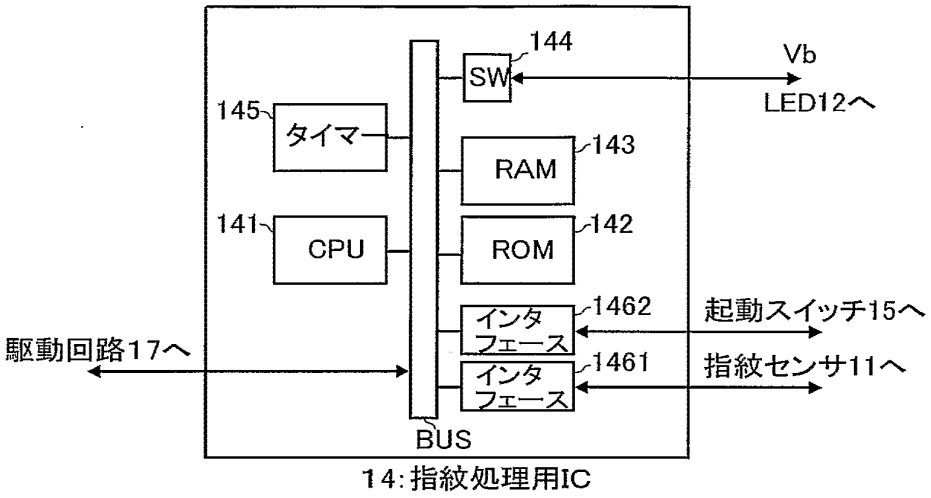


(A)



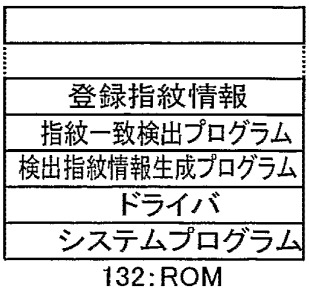
(B)

図7



14:指紋処理用IC

(A)



132:ROM

(B)

図8

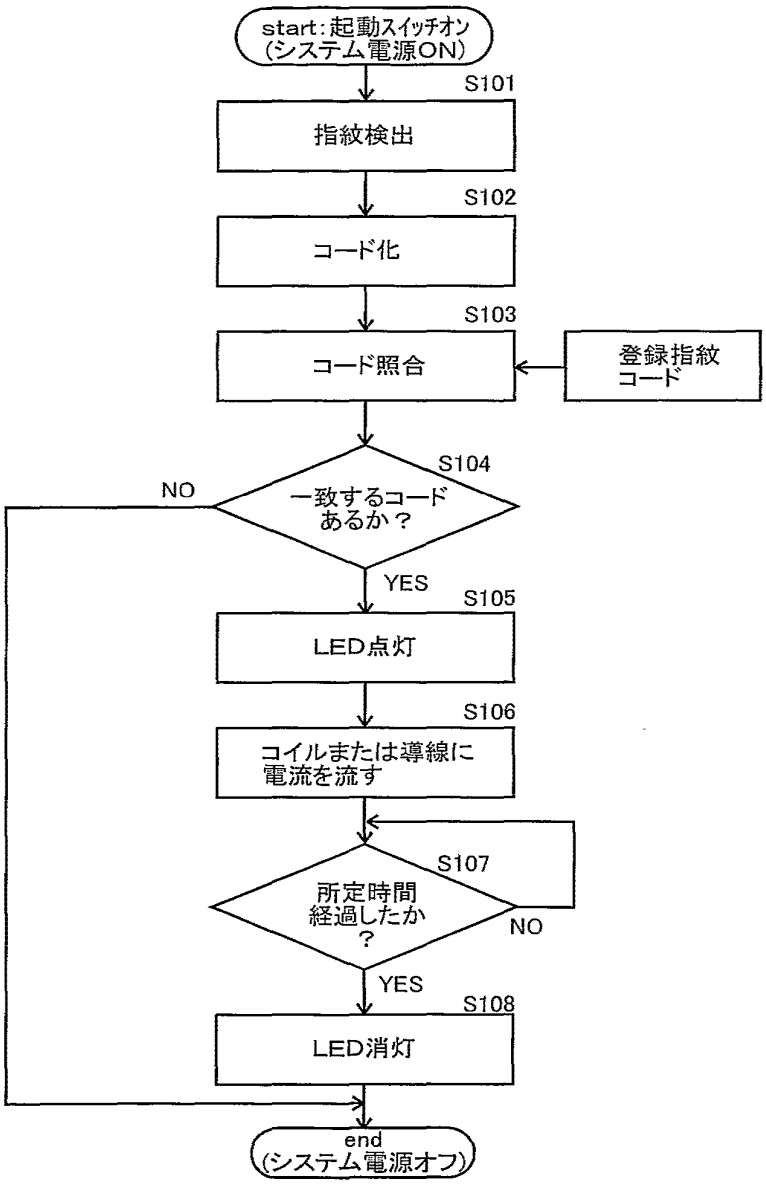
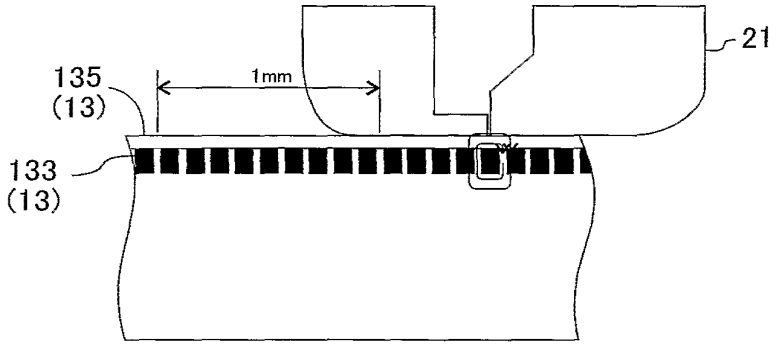
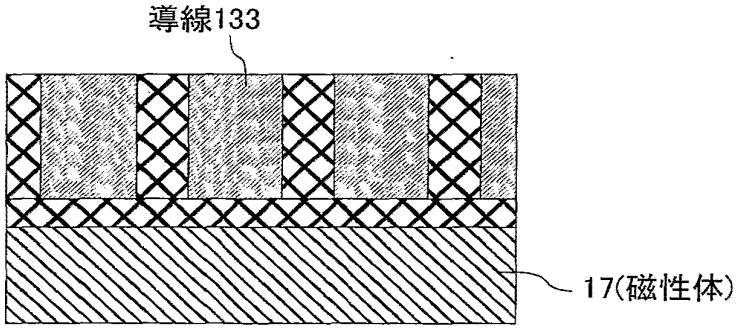

start:起動スイッチオン
(システム電源ON)
S101
指紋検出
S102
コード化
S103
コード照合
登録指紋
コード
S104
一致するコード
あるか？
NO
YES
S105
LED点灯
S106
コイルまたは導線に
電流を流す
S107
所定時間
経過したか
？
NO
YES
S108
LED消灯
end
(システム電源オフ)

図9

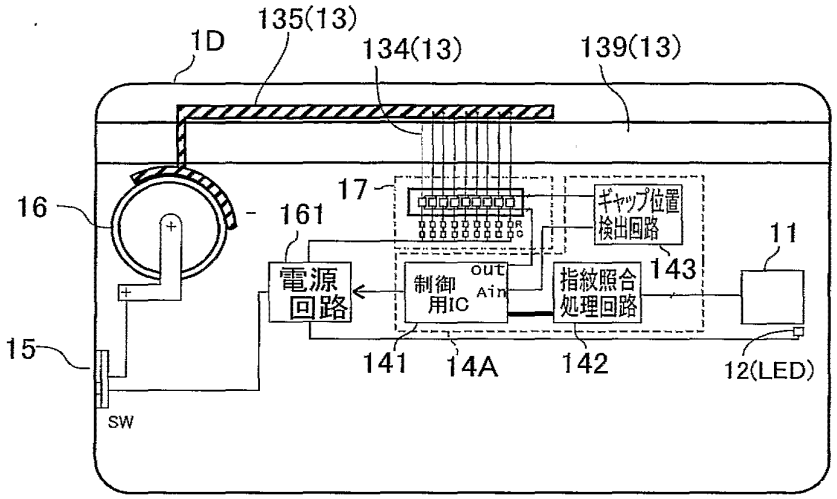


(A)

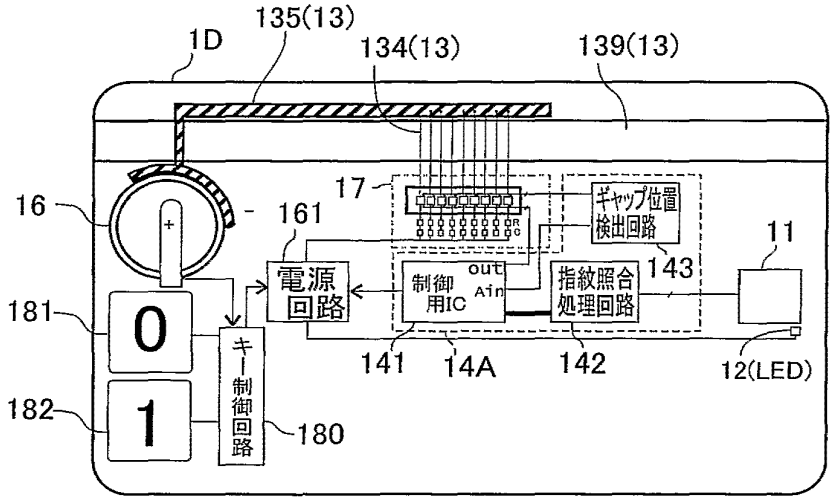


(B)

図10

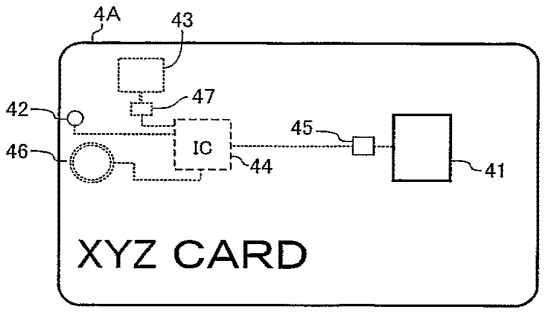

1D
135(13)
134(13)
139(13)
16
17
161
ギャップ位置検出回路
11
143
電源回路
制御用IC
out
Ain
指紋照合処理回路
15
141
14A
142
12(LED)
SW

(A)

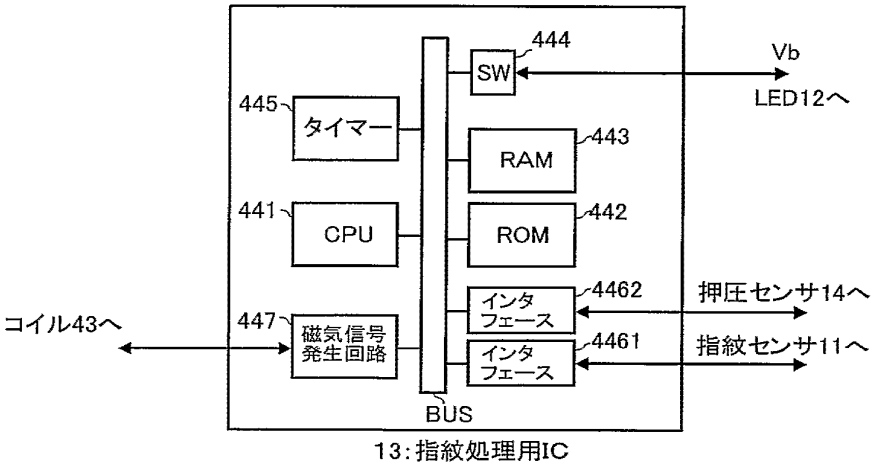

1D
135(13)
134(13)
139(13)
16
17
161
ギャップ位置検出回路
11
143
電源回路
制御用IC
out
Ain
指紋照合処理回路
181
0
1
182
キー制御回路
180
141
14A
142
12(LED)

(B)

図11


4A
43
47
42
IC
45
46
44
41
XYZ CARD

(A)


444
SW
Vb
LED12へ
445
タイマー
443
RAM
441
CPU
442
ROM
4462
インタフェース
押圧センサ14へ
コイル43へ
447
磁気信号発生回路
4461
インタフェース
指紋センサ11へ
BUS
13:指紋処理用IC

(B)

図12

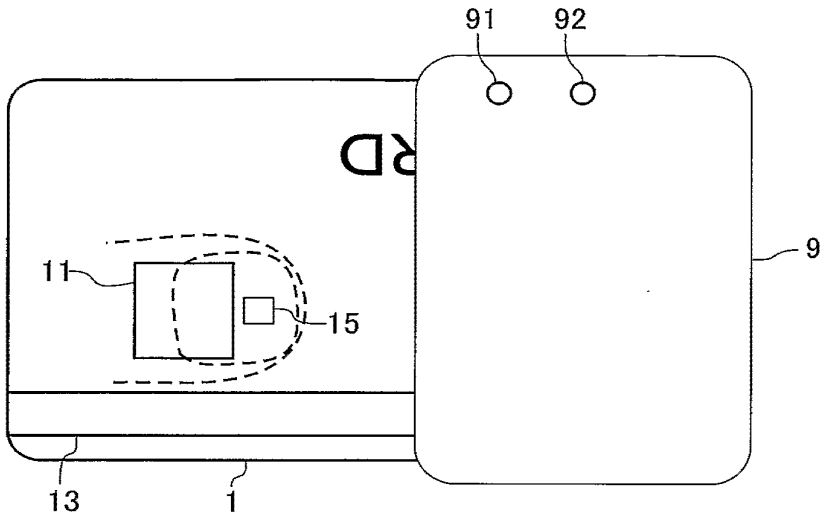
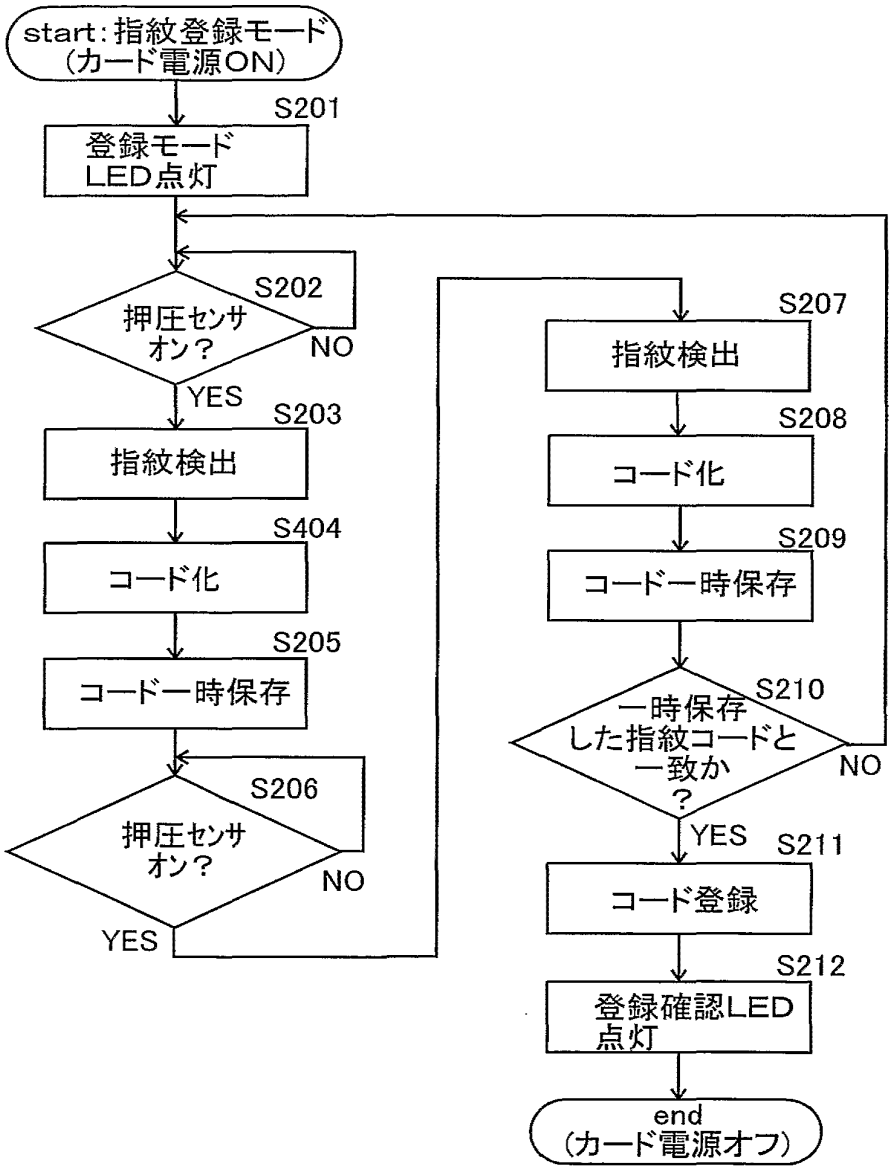


図13


start：指紋登録モード
（カード電源ON）
S201
登録モード
LED点灯
S202
押圧センサ
オン？
NO
YES
S203
指紋検出
S404
コード化
S205
コード一時保存
S206
押圧センサ
オン？
NO
YES
S207
指紋検出
S208
コード化
S209
コード一時保存
S210
一時保存
した指紋コードと
一致か
？
NO
YES
S211
コード登録
S212
登録確認LED
点灯
end
（カード電源オフ）

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/013473

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06K19/00, G06T7/00, B42D15/10

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)
Int.Cl[7] G06K19/00, B42D15/10

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

Jitsuyo Shinan Koho	1922-1996	Jitsuyo Shinan Toroku Koho	1996-2004
Kokai Jitsuyo Shinan Koho	1971-2004	Toroku Jitsuyo Shinan Koho	1994-2004

Electronic data base consulted during the international search (name of data base and, where practicable, 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	JP 59-202581 A (Mitsubishi Electric Corp.), 16 November, 1984 (16.11.84), Full text; all drawings (Family: none)	1-4,11-14 5-10,15-18
X	JP 3-136899 A (Hirokazu NAKANO), 11 June, 1991 (11.06.91), Full text; all drawings (Family: none)	1-4,11-14
X	JP 9-305724 A (Tamura Electric Works, Ltd.), 28 November, 1997 (28.11.97), Full text; all drawings (Family: none)	1-4,11-14

☐ 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 08 October, 2004 (08.10.04)	Date of mailing of the international search report 26 October, 2004 (26.10.04)
Name and mailing address of the ISA/ Japanese Patent Office Facsimile No.	Authorized officer Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００４／０１３４７３

Ａ．　発明の属する分野の分類（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷ Ｇ０６Ｋ１９／００，Ｇ０６Ｔ７／００，Ｂ４２Ｄ１５／１０

Ｂ．　調査を行った分野

調査を行った最小限資料（国際特許分類（ＩＰＣ））

Ｉｎｔ．Ｃｌ⁷ Ｇ０６Ｋ１９／００，Ｂ４２Ｄ１５／１０

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　　１９２２－１９９６年
日本国公開実用新案公報　１９７１－２００４年
日本国実用新案登録公報　１９９６－２００４年
日本国登録実用新案公報　１９９４－２００４年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

Ｃ．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Ｘ	ＪＰ　５９－２０２５８１　Ａ（三菱電機株式会社） １９８４．１１．１６，全文，全図（ファミリーなし）	1－4，11－14
Ａ		5－10，15－18
Ｘ	ＪＰ　３－１３６８９９　Ａ（中野　浩和） １９９１．０６．１１，全文，全図（ファミリーなし）	1－4，11－14
Ｘ	ＪＰ　９－３０５７２４　Ａ（株式会社田村電機製作所） １９９７．１１．２８，全文，全図（ファミリーなし）	1－4，11－14

☐ Ｃ欄の続きにも文献が列挙されている。　　☐ パテントファミリーに関する別紙を参照。

＊　引用文献のカテゴリー
「Ａ」特に関連のある文献ではなく、一般的技術水準を示すもの
「Ｅ」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「Ｌ」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「Ｏ」口頭による開示、使用、展示等に言及する文献
「Ｐ」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「Ｔ」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「Ｘ」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Ｙ」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「＆」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
０８．１０．２００４	26.10.2004

国際調査機関の名称及びあて先	特許庁審査官（権限のある職員）	５Ｂ	８６２７
日本国特許庁（ＩＳＡ／ＪＰ） 郵便番号１００－８９１５ 東京都千代田区霞が関三丁目４番３号	大塚　良平 電話番号　０３－３５８１－１１０１　内線　３５４６		

様式ＰＣＴ／ＩＳＡ／２１０（第２ページ）（２００４年１月）

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 December 2005 (15.12.2005)

PCT

(10) International Publication Number
WO 2005/119607 A3

(51) International Patent Classification:
G07F 19/00 (2006.01) *G07F 7/10* (2006.01)

(21) International Application Number:
PCT/US2005/019988

(22) International Filing Date: 3 June 2005 (03.06.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/576,894 3 June 2004 (03.06.2004) US
60/591,998 28 July 2004 (28.07.2004) US

(71) Applicant *(for all designated States except US)*: **TYFONE, INC.** [US/US]; 1490 Clifton Street, Portland, Oregon 97201 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SPITZER, Thomas N.** [US/US]; 1490 Clifton Street, Portland, Oregon 97201 (US). **TADEPALLI, Prabhakar** [US/IN]; 290 Phase II, Adarsh Palm Meadows, Airport Whitefield Road, Bangalore, Karnataka 560066 (IN). **NARENDRA, Siva G.** [IN/US]; 7180 SW 84th Avenue, Portland, Oregon 97223 (US).

(74) Agent: **LEMOINE, Dana B.**; LeMoine Patent Services, PLLC, c/o Portfolio IP, P.O. Box 52050, Minneapolis, Minnesota 52050 (US).

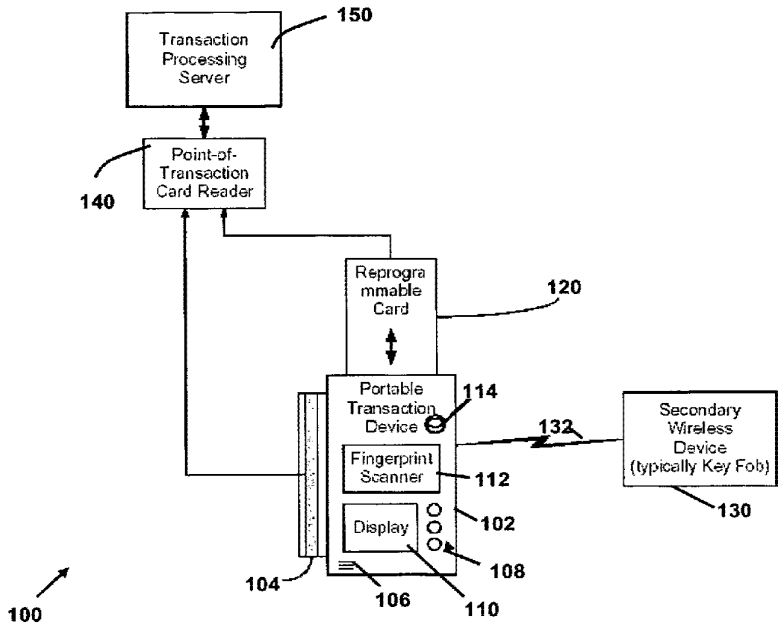
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, 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, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, 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).

Published:
— *with international search report*

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR SECURING FINANCIAL TRANSACTIONS



(57) Abstract: A financial transaction system utilizes multi-factor authentication to secure financial transactions. The system comprises a portable transaction device (e.g. a wireless phone) which is used to program the magnetically or electronically reprogrammable stripe of a magnetic stripe card or the memory of a smart card. A single-use account number may be used to program the card. The device provides biometric authentication and secondary authentication using a secondary wireless device. The device and the programmed cards are used in various financial transactions.

WO 2005/119607 A3

(88) Date of publication of the international search report:
4 May 2006

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.

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US2005/019988

A. CLASSIFICATION OF SUBJECT MATTER
G07F19/00 G07F7/10

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)
G06K G06F G07F

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 016 476 A (MAES ET AL) 18 January 2000 (2000-01-18) column 2, line 21 - column 4, line 22 column 4, line 65 - column 15, line 25 figures -----	1-11
Y	US 2003/220876 A1 (BURGER TODD O ET AL) 27 November 2003 (2003-11-27) page 5, paragraph 93 - page 22, paragraph 313 figures 1-11 -----	1-11
Y	US 2003/080183 A1 (RAJASEKARAN SANGUTHEVAR ET AL) 1 May 2003 (2003-05-01) page 1, paragraph 2 - page 3, paragraph 19 page 3, paragraph 35 - page 4, paragraph 41 figures 4,5 -----	1-11
	-/--	

[X] Further documents are listed in the continuation of box C.

[X] 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	Date of mailing of the international search report
2 December 2005	16 DEC 2005

Name and mailing address of the ISA	Authorized officer
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	Rachkov, V

Form PCT/ISA/210 (second sheet) (January 2004)

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 December 2005 (15.12.2005)

PCT

(10) International Publication Number
WO 2005/119607 A2

(51) International Patent Classification[7]: G07F 19/00

(21) International Application Number: PCT/US2005/019988

(22) International Filing Date: 3 June 2005 (03.06.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/576,894 3 June 2004 (03.06.2004) US
60/591,998 28 July 2004 (28.07.2004) US

(71) Applicant *(for all designated States except US)*: **TYFONE, INC.** [US/US]; 1490 Clifton Street, Portland, Oregon 97201 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SPITZER, Thomas N.** [US/US]; 1490 Clifton Street, Portland, Oregon 97201 (US). **TADEPALLI, Prabhakar** [US/IN]; 290 Phase II, Adarsh Palm Meadows, Airport Whitefield Road, Bangalore, Karnataka 560066 (IN). **NARENDRA, Siva G.** [IN/US]; 7180 SW 84th Avenue, Portland, Oregon 97223 (US).

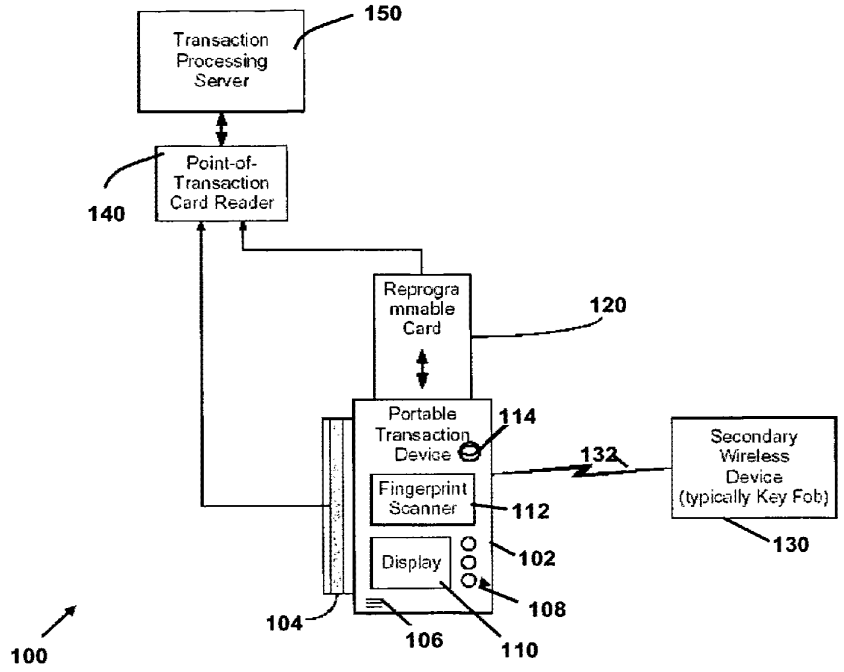
(74) Agent: **LEMOINE, Dana B.**; LeMoine Patent Services, PLLC, c/o Portfolio IP, P.O. Box 52050, Minneapolis, Minnesota 52050 (US).

(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, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, 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, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, 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).

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR SECURING FINANCIAL TRANSACTIONS



(57) Abstract: A financial transaction system utilizes multi-factor authentication to secure financial transactions.

WO 2005/119607 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.

SYSTEM AND METHOD FOR SECURING FINANCIAL TRANSACTIONS

Field

The present invention relates generally to portable transaction devices, and more specifically to portable transaction devices having various security features.

Background

Instances of financial card fraud and identity theft have increased dramatically in recent years, particularly with the rapid increase of online and electronic transactions. Solutions of varying efficacy have been proposed to protect financial information and otherwise guard against fraud and theft. Firewalls protect computer systems against unauthorized access; however, they cannot be completely assured of the identities of individuals accessing the network. Various electronic devices may be employed to verify the identity of individuals; however, these devices often permit authentication information to be accessed. Some systems provide significantly improved security, but at the expense of requiring substantial changes to point-of-sale devices or other parts of the transactional infrastructure.

Brief Description of the Drawings

Figures 1 and 2 show transaction systems with multi-factor authentication;

Figure 3 shows a block diagram of a programmable card;

Figure 4 shows a block diagram of a secondary wireless device;

Figure 5 shows a computer and base station;

Figure 6 shows usage models for various embodiments of the present invention;

Figure 7 shows an intelligent electronic device capable of printing checks;

Figures 8-10 show various methods for financial card transaction verification in accordance with various embodiments of the present invention;

Figure 11 shows a flexible form factor for a programmable financial card;

Figure 12 shows an exploded perspective view of the programmable financial card of Figure 11;

Figure 13 shows usage models for a secondary wireless device in card-present transactions and card-not-present transactions;

Figure 14 shows an architecture diagram for a transaction system with multi-factor authentication;

Figure 15 shows usage models for electronic money transfer;

Figure 16 shows usage models for pre-paid card recharge; and

Figure 17 shows business methods.

Description of Embodiments

In the following detailed description, reference is made to the accompanying drawings that show, by way of illustration, various embodiments of an invention. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention. It is to be understood that the various embodiments of the invention, although different, are not necessarily mutually exclusive. For example, a particular feature, structure, or characteristic described in connection with one embodiment may be implemented within other embodiments without departing from the spirit and scope of the invention. In addition, it is to be understood that the location or arrangement of individual elements within each disclosed embodiment may be modified without departing from the spirit and scope of the invention. The following detailed description is, therefore, not to be taken in a limiting sense, and the scope of the present invention is defined only by the appended claims, appropriately interpreted, along with the full range of equivalents to which the claims are entitled. In the drawings, like numerals refer to the same or similar functionality throughout the several views.

The present disclosure relates generally to use of a portable transaction device having various security features. The security features may be employed to particular advantage in financial transactions, so as to enhance security beyond that currently available in transactions conducted with financial cards,

IPR2025-00644 Page 01088

bank checks and existing computing devices. Traditionally, financial cards have information physically present on the front face and in the magnetic stripe. Similarly, bank account number, account holder's name, routing number and the address are present in the face of the checks. If a financial card or a checkbook is lost or stolen, or if the card is skimmed (an unauthorized swipe to gather card holder information stored on the stripe), the information is insecure and is available for use by anyone. Similar risks are present with computing devices and other electronic devices used in financial transactions.

Accordingly, as shown in Fig. 1, a transaction system 100 with multi-factor authentication may be employed. As shown in this embodiment, the system 100 may include: a central transaction processing server 150; a point-of-sale transaction card reader 140; a portable transaction device 102 for use in credit/debit card type transactions; a key fob or other secondary wireless device 130 configured to wirelessly communicate with the portable transaction device 102; a reprogrammable card 120 that may be inserted into the portable transaction device 102 and reprogrammed with a one-time use transaction number or a reprogrammable electronic stripe 104 attached directly to the portable transaction device 102.

The portable transaction device 102 may include a camera (video and picture) component 114, a biometric (e.g., fingerprint) scanner 112, a display 110, a voice (microphone and speaker) component 106, and controls 108. The portable transaction device 102 may also include voice-activation and camera functionality. The secondary wireless device 130 may communicate wirelessly with the portable transaction device 102 using any type of wireless communications protocol. For example, the secondary wireless device 130 and the portable transaction device 102 may communicate using a Bluetooth type wireless link 132.

Where a one-time use transaction number is employed, the number may be generated by the card issuer or locally by the portable transaction device 102. Generation of the single-use number may be accomplished in one of several ways. For example, when an account is issued the card holder may get several pre-assigned surrogate numbers. The numbers will also have a pre-specified sequence. This sequence is known to the issuing bank and the user's portable

transaction device 102. The issuing bank will authorize payments only based on the expected sequence of account numbers. If out-of-sequence account numbers are used, then the issuing bank will consider that transaction as a potential theft. The issuing bank can also use this feature to track the merchant involved in the potentially fraudulent transaction.

According to another example, a pre-assigned sequence can be reset to the original starting number on the list depending on user input or other triggers. In addition, the list of numbers can be downloaded via the mobile phone network on a regular basis. This can enhance security by minimizing the potential for repetitive number lists.

Regardless of the particular method, upon receipt of the surrogate card number, the merchant typically sends the surrogate card number to the card issuer for authorization/validation. Merchants do not need to install additional software to receive surrogate card numbers or to transmit them to card issuers. When the card issuer receives the account number, it is flagged as a single-use number and decoded to reveal the cardholder's standing account number. An authorization or denial is attached to the account number, which is recoded back to the temporary account number and sent to the merchant. Any attempt to reuse a surrogate card number outside the parameter results in denied authorization. In addition to or instead of these examples, other methods for generating one-time use numbers may be employed.

In conducting a transaction, the user, possessing both the secondary wireless device 130 and the portable transaction device 102, may press a control button 108 on the portable transaction device 102 requesting that the card 120 or electronic stripe 104 be readied with a new one-time use transaction number. The electronic stripe 104 may be selected by the user for use in swipe-type card readers, and the card 120 may be selected for either swipe-type card readers or insertion-type card readers, such as ATMs. It will be appreciated that the device 102 may be manufactured with only an electronic stripe, or only a card reader, rather than both. It will be further appreciated that the card 120 may include a reprogrammable magnetic stripe, a reprogrammable electronic stripe, or may be a so-called "smart" card with a reprogrammable internal memory, and the

portable transaction device 102 may be configured to interface and reprogram one or more of these types of cards.

It should be appreciated that the portable transaction device 102 may be implemented in a variety of different configurations. For example, as described at length below and shown below in an alternate system depiction (Fig. 2), the portable transaction device may be implemented as, or in connection with, a mobile telephone.

Fig. 2 shows a transaction system with multi-factor authentication. Transaction system 200 includes transaction processing server 150, point-of-sale (POS) transaction card reader 140, mobile telephone 202, removable and reprogrammable card 205, and secondary wireless device 130. Mobile telephone 202 is an example of a portable transaction device, and any reference made herein to a portable transaction device is meant to include mobile telephones as well as other portable transaction device embodiments.

The mobile telephone 202 may include a camera (video and picture) component 114, a biometric (e.g., fingerprint) scanner 112, a display 110, a voice (microphone and speaker) component 106, and controls 108. The mobile telephone 202 may also include voice-activation and camera functionality. The secondary wireless device 130 may communicate wirelessly with the mobile telephone 202 using any type of wireless communications protocol. For example, the secondary wireless device 130 and the mobile telephone 202 may communicate using a Bluetooth type wireless link 132. Further, the mobile telephone may communicate with a cell network, shown by signal 232.

Removable and reprogrammable card 205 may be utilized in many ways. For example, removable and reprogrammable card 205 may be left in the mobile telephone 202 for use in swipe-type card readers, or may be removed from mobile telephone 202 for use with insertion-type card readers. Examples of insertion-type card readers include automatic teller machines (ATMs).

In the example of Fig. 2, the mobile phone 202 provides all the functionality of the previously-described portable transaction device 102 (Fig. 1). In addition, the ability of the mobile phone 202 to access a communications network (e.g., the cell phone network) may be used to provide additional functionality. For example, if the cell phone is lost, a call can be placed through

the network to disable all financial card functions. If the key fob is lost, a new key fob can be mailed to the user and the configuration information can be updated automatically by placing a call through the cell phone network.

Regardless of the particular configuration, the system may be configured to eliminate or reduce fraudulent transactions by performing multiple authentications of each transaction, as follows. Possession of the portable transaction device provides a first factor of authentication. Second, the fingerprint of the user may be scanned and checked against a fingerprint stored in memory on the device. Third, at the time of the transaction, the wireless link to the secondary wireless device may be checked to verify that the secondary wireless device is communicating a proper device ID to the portable transaction device, thus indicating that the secondary wireless device is located within a predetermined distance of the portable transaction device. If these authentication steps are satisfied, the electronic stripe or card is reprogrammed with a one time use transaction number. In addition, the portable electronic device may store information pertaining to multiple different cards, and the user would be allowed to supply an input specifying which of the cards would be designated for use in the upcoming transaction.

Once the card is readied for use after authentication and any required user input, the user or a store clerk may swipe the electronic stripe through a swipe-type card reader, remove the card from the device and swipe it in a swipe-type card reader, or feed it into an insertion-type card reader, such as found on an ATM. As an additional authentication step, the one-time use transaction number may be checked by the transaction processing server for validity.

As described above, various embodiments of the present invention provide multi-factor authentication. For example, various embodiments of the invention may use two or three factor authentication for access control and information or identity theft prevention of financial card, bank check, electronic and computing devices. Two-factor authentication is defined as providing access based on validating whether the user has access to at least two verifiable pieces of information that are truthful and are available only to him/her. An example of two factor authentication is having access to a debit card and knowing the correct PIN number to complete a debit card transaction. Similarly,

three-factor authentication is defined as providing access based on validating whether the user has access to at least three verifiable pieces of information that are truthful and are available only to him/her.

The following is an outline of various system elements that may be used in implemented various embodiments of the described systems and methods. It will be appreciated that no single element is essential to every possible exemplary embodiment.

1. Portable transaction device (e.g., portable telephone)

A. Wireless interface configured to detect secondary wireless device when within predetermined distance (e.g. Bluetooth)

B. Fingerprint scanner

C. Memory storing fingerprint data of authorized user

D. Display (optional)

E. Controls for reprogramming card/stripe

F. Card insertion slot

G. Electronically reprogrammable stripe

H. Camera functionality: when the portable transaction device is activated, a photograph of the user may be taken. The photograph may be send to the card issuer and/or displayed on the portable transaction device during use to provide additional security (e.g., a fourth authentication factor)

I. Voice-activation functionality

2. Wireless secondary device (e.g. key fob)

A. Wireless link to portable transaction device

3. Card

A. Magnetically programmable stripe OR electronically programmable stripe, OR electronically programmable internal memory (so called smart card)

B. Configured to be inserted into portable transaction device and programmed with a one-time use card number on a per-transaction basis

4. Point of Transaction Card Reader

5. Transaction Processing Server

6. Authentication factors (may be implemented in varying combinations) to determine if a pending transaction is fraudulent

A. Wireless secondary device within predetermined range of portable transaction device

B. Scanned fingerprint matches stored fingerprint

C. Single-use transaction number written to card is valid

The financial transaction system and portable electronic device described herein may be advantageously employed in various settings in addition to or instead of those already described. Discussed below are various additional usage models and settings under the headings "Quicker time-to-market software only solution," "Combined electronic cards and software solutions," and "Personal money management."

1. Quicker time-to-market software only solution

Single-use number software installed on any mobile phone can help with securing card-not present transactions and can extend the idea initiated by Verified-By-VISA to all mobile phone users, thereby increasing the security of e&m-commerce transactions almost immediately. Various software embodiments of the present invention, along with already existing mobile infrastructure such as cameras on phones, SMS & MMS, and GPRS may be used effectively to increase e-commerce, and m-commerce.

2. Combined electronic cards and software solutions

Various embodiments of the present invention that include electronic stripe cards or smartcards may be used for the following:

A. Customers can inform his/her bank of a certain charge limit, beyond which the user would have to provide additional security through SMS message before the transaction can be completed.

B. A service provider may locate a customer by identifying the phone through the current network it is operating in. Since the card is integrated into the phone, a card being used outside its typical usage area can be readily identified. If it is being used in a "negative list" area, for example, the bank can confirm user authenticity with the user using SMS or mobile call. As an added value, once user authenticity is confirmed, locations of ATMs and merchant promotions can be sent directly to the user at his/her request.

C. To recharge stored-value/prepaid cards on the fly, by extending m-banking to the payment transaction level.

D. Be a money exchange mechanism between individuals by using the VISA or MasterCard authentication networks, i.e. replace services like Western Union with more convenient m-banking, m-cashing networks. Where POS installations are in their infancy, card issuing banks and merchant banks can reap value from mobile-to-mobile transactions while not compromising the integrity of their existing transaction mechanisms.

E. Provide more convenience and control to VisaBuxx customer segments by allowing users transparency to their secondary and tertiary cards, provide limits to transactions beyond which the primary card-holder needs to approve and have the ability to recharge the secondary and tertiary cards when pre-determined levels are reached.

F. Provide entry level prepaid cards/phones to "Teens" while employing budgetary controls (as in debit cards).

G. Use camera, fingerprint, and voice for authentication of card-present transactions.

H. Where appropriate, combine loyalty/incentive programs with cards, minutes used thereby align interest with the SmartCard program.

I. Where appropriate, use Infra-red, Bluetooth, or other wireless payments schemas to help banks get direct control of contactless payment paradigms.

3. Personal Money Management

Voice modules on phones can be used to record transactions and where pertinent, the transactions can be downloaded into money management software. This eliminates the hassle of having to type out all transactions and, as bandwidth improves, allows the customer to compare transactions with bank statements.

Figure 3 shows a block diagram of a programmable card. Programmable card 300 may be utilized as removable and reprogrammable card 205 (Figure 2). Programmable card 300 includes thin profile battery 302, power management circuitry 304, microcontroller with flash 306, Bluetooth front end 310, Bluetooth

antenna 312, universal serial bus (USB) and power supply connector 322, and display driver 320.

Figure 4 shows a block diagram of a secondary wireless device. Secondary wireless device 400 may be utilized as secondary wireless device 130 (Figures 1, 2). Secondary wireless device 400 includes thin profile battery 402, power management circuitry 404, microcontroller 406, read only memory (ROM) 420, FLASH memory 408, Bluetooth front end 410, Bluetooth antenna 412, and USB and power supply connector 422.

Figure 5 shows a computer and base station. Computer 510 may be any type of computer or computing device capable of being operated by a user and being coupled to base station 520. For example, computer 510 may be a personal computer, a handheld computer, or the like. Computer 510 may include software to drive the base station and its components, and may also include graphical user interface (GUI) front end software for step-by-step user instructions for programming a reprogrammable card. As described above, programming a reprogrammable card may include selection of rolling numbers and associated maximum transaction amounts.

As shown in Figure 5, base station 520 includes universal serial bus (USB) interface 528, card reader 522, secondary wireless device slot 526, and a reprogrammable card slot 524. Base station 520 may communicate with computer 510 over a cable coupled to USB interface 528. Although interface 528 is shown as a USB interface, this is not a limitation of the present invention. Any suitable interface may be used without departing from the scope of the present invention.

Base station 520 provides an interface between computer 510 and one or more other items. For example, in some embodiments, a reprogrammable card may be placed in slot 524 for communications with computer 510, or for programming by computer 510. Further, in some embodiments, a secondary wireless device may be placed in slot 536 for communications with computer 510, or for programming by computer 510. Also in some embodiments, base station 520 may be used for charging a reprogrammable card and secondary wireless device.

Base station 520 may also be used for reading standard magnetic cards to store information into a reprogrammable card. For example, a reprogrammable card may be placed in slot 524, and one or more standard magnetic cards may be swiped through card reader 522. Base station 520 may include circuitry to program a reprogrammable card directly from swiped magnetic cards, or may program a reprogrammable card under the control of computer 510.

Figure 6 shows usage models for various embodiments of the present invention. Figure 6 shows user icons to represent users in various stages of use, and arrows to indicate actions. The various usage models are now described. At 602, an un-programmed reprogrammable card, a secondary wireless device, and a base station are shipped to a user. Software on CD-ROM and an optional travel kit may also be shipped to the user. At 604, the user 612 installs the software and connects the base station to a home personal computer (PC). The software is run to initiate programming, and the user scans a fingerprint into the reprogrammable card. The user plugs the reprogrammable card and the secondary wireless device into the base station.

At 614, the software communicates with a server 622 to activate the reprogrammable card and secondary wireless device. Server 622 may be held at a secure location separate from the user and from a card issuing bank 660. For example, server 622 may be held by a company that provides reprogrammable cards and secondary wireless devices. Further, information may be stored on the server 622 for retrieval in case of loss of the reprogrammable card or secondary wireless device. The user 612 may then scan one credit card at a time into the base station. This may be repeated any number of times. The user 612 is shown at a PC performing the actions just described.

At 618, the user 642 has completed the setup, and has a reprogrammable card available for use. The user 642 carries both the reprogrammable card and the secondary wireless device. It is best to keep the secondary wireless card separate from the reprogrammable card. The secondary wireless device never has to be accessed by user 642 to initiate a transaction. At the end of the day, the user 642 plugs the reprogrammable card and the secondary wireless device into the base station for charging and account summary.

At 644, user 670 initiates a transaction with merchant 672. To initiate the transaction, user 670 activates the reprogrammable card using a fingerprint scan and selects the credit card to use. The reprogrammable card authenticates only in the presence of the appropriate secondary wireless device. Information programmed on the reprogrammable card's electronic stripe will get erased automatically after a predetermined timeout. For example, the information may get erased after five minutes. To prevent multiple swipes, the information in the reprogrammable card may be erased after one swipe. An alternative is to provide a rolling account number that the credit card company can map to the actual account number. The account number may then roll to a new number for each fingerprint scan.

If a user 652 loses one of the reprogrammable card or secondary wireless device, shown by 654, the company will mail a preprogrammed reprogrammable card or secondary wireless device to the user 652 at 624. If a user 632 loses both the reprogrammable card and secondary wireless device, shown by 616, the company will help deactivate all user credit card accounts and start the process again at 634.

As described above, reprogrammable cards may take any suitable form. For example, reprogrammable cards may be magnetic stripe cards, electronically programmable cards, smart cards, or any combination. Various embodiments are now described under headings relating to magnetic cards, electrically programmable cards, and smart cards. It should be noted that nothing in these embodiments should be considered essential.

Magnetic stripe cards

Embodiments that include magnetic stripe cards are now described with reference to Figures 1-6. Various embodiments of the present invention include: (i) an intelligent (memory, computational power) electronic device that has magnetic stripe reading / writing capability, and a wireless link such as Bluetooth; (ii) a fingerprint scanner on the intelligent electronic device; (iii) electronic device such as a key that has memory and wireless connection such as Bluetooth; and (iii) an empty generic three track magnetic stripe card that can be programmed by the intelligent electronic device on a per transaction basis. For

example, Figures 1 and 2 show portable transaction devices 102 and 202 that may be used as intelligent electronic devices. Further, portable transaction devices 102 and 202 are shown having wireless links and fingerprint scanners. Portable transaction device 202 is shown having a magnetic stripe reader/writer to program reprogrammable card 205.

The use of an intelligent electronic device with a fingerprint scanner or the use of an intelligent electronic device and the key (secondary wireless device) constitutes a two-factor authentication solution while the use of all three (intelligent electronic device with the fingerprint scanner and the key) constitutes a three-factor authentication solution.

The user first installs interface software in the intelligent electronic device. Using the installed software the user scans his/her portfolio of standard financial cards using the integrated magnetic stripe card reader. The user may also enter information necessary for financial card transactions that may not be present in the magnetic stripe such as a security code. The user also scans a fingerprint to associate the cards with the user. The financial card information is stored in the intelligent electronic device in encrypted form. The decryption code for the information stored in the intelligent electronic device may be stored in the key. Each intelligent electronic device may have an associated key that is unique. Once all the relevant information is stored in the intelligent electronic device, the user may slide the generic card into the integrated magnetic stripe reader/writer.

When the user is ready to use a financial card for a transaction s/he logs into the intelligent electronic device using the fingerprint scanning device or by entering a password. In the two-factor solution, the card user can proceed with initiating the transaction. In the case where the user opts for a three-factor solution, the intelligent electronic device will let the login occur only if it is able to establish a wireless link with its associated key. The user then selects the type of card to use. After log in using either approach, the intelligent electronic device receives the decryption code from the key to access the information about the selected card, if key based authentication is used. If fingerprint scan based authentication is used for two-factor then the decryption code is stored in the intelligent electronic device itself, which will be provided after the

authentication. The user then pulls out the generic card, during which the card is programmed by the magnetic writer. At this point the intelligent electronic device deletes the decryption key information that it received from the key. Once programmed, the generic card can be used like any other magnetic stripe financial card. Once the transaction is completed the user inserts the card back into the intelligent electronic device during which the information stored in the magnetic stripe is erased.

Further embodiments may be generated by combining various feature of magnetic card embodiments with electronically programmable embodiments and smart card embodiments, described below. The use of magnetic cards as reprogrammable cards may obviate the need for a power supply in the card, and provides a mechanism to use traditional three track magnetic stripe cards and hence does not require development of a card that has an alternate programming medium.

Note that the need for having access to the intelligent electronic device along with fingerprint scanning and the presence of a key provides a three-factor authentication. The same can be implemented without the key in which case the security of the information stored in the intelligent electronic device may be achieved with two-factor authentication through fingerprint scanning. The key can also be replaced with a PIN input + fingerprint scanning; however, without the key the decryption code is physically stored in the same device as that of the information. A key along with the intelligent electronic device can be used as two-factor authentication.

Electronically programmed cards

Embodiments that include electronically programmable cards are now described with reference to Figures 1-6. Various embodiments of the present invention include: (i) a base station having the ability to scan a user's card information; (ii) an electronic card that has an electronically programmable region that has identical dimensions as that of a magnetic stripe (henceforth referred to as the electronic stripe), a wireless link such as Bluetooth and a fingerprint scanner; (iii) an electronic device such as a key that has memory and a wireless link such as Bluetooth. For example, Figures 1 and 2 show portable

transaction devices 102 and 202 that may be used as intelligent electronic devices. Further, stripe 104 (Figure 1) may be a reprogrammable electronic stripe, and stripe 204 (Figure 2) may be a reprogrammable electronic stripe. Note that the electronic programming may be done using electric currents. The direction of current travel will change the magnetic field and hence can be used to code for a digital "1" or a digital "0". This information can then be read by a traditional magnetic stripe reader present in point-of-sale.

The electronic card may come preprogrammed with software that will allow users to input card information or the users may first install interface software in the intelligent electronic device or in the base station. Using the installed software the user will then enter standard financial card information. An optional card reader can be used to read most of the information present in a financial card. The financial card information will be stored in the intelligent electronic device in encrypted form. The decryption code for the information stored in the intelligent electronic device will be stored in the key. Each intelligent electronic device will have an associated key that is unique.

When the user is ready to use a financial card for a transaction s/he logs into the intelligent electronic device using a fingerprint scanning device or by entering a password. In the two-factor solution, the card user can proceed with initiating the transaction. In the case where the user opts for a three-factor solution, the intelligent electronic device will let the login occur only if it is able to establish a wireless link with its associated key. The user then selects the card to use through a card selection button on the face of the intelligent electronic device. The intelligent electronic device receives the decryption code from the key to access the information about the selected card. The intelligent electronic device programs the electronic stripe. At this point the intelligent electronic device deletes the decryption key information that it received from the key. Once programmed the intelligent electronic device can be used like any other magnetic stripe financial card. Once the transaction is completed, the intelligent electronic device erases the information stored in the electronic stripe. The electronic stripe can be programmed to time out after a certain length of time or after a specified number of swipes.

In some embodiments, the key may store all critical information from the intelligent electronic device as backup in encrypted format. The decryption code for information stored in the key may be present in its associated intelligent electronic device. Also in some embodiments, an intelligent electronic device may include software having the ability for the intelligent electronic device to either limit to one swipe after programming or record how many times a card was swiped between magnetic stripe programming and erasing. In further embodiments, the intelligent electronic device may include software and/or voice recognition that tracks the expenses based on user input every time the card is used or when the user makes any expense transaction to provide categorized expense summary. In further embodiments, the intelligent electronic device may include the ability to communicate to the point-of-sale the amount entered by the user for transaction – this however will require change to the point-of-sale. In still further embodiments, the intelligent electronic device may include the ability to generate one account number from a set of account numbers. These numbers will be generated in a predetermined sequence (or one time use numbers) that will expire at the end of every transaction to eliminate card cloning and counterfeiting operations. In some embodiments, this may be achieved by either using the 19 digit PAN Field and/or Discretionary Data character fields allocated in the magnetic stripe standards. For example, the way the variable number (required for off-line transactions) would work is that a card holder may be assigned let us say 100 account numbers. The account numbers will revolve in a pre-determined order. The issuing bank will know what order will be used and so will the intelligent electronic device. For each authentication the intelligent electronic device will activate one number in the pre-determined order. The variable number also applies for on-line transactions and can either replace or work with the one time use numbers.

In some embodiments, the programmed magnetic stripe may be detached from the main unit for use in transactions where the card is swallowed in whole to complete the transaction (such as in an ATM machine or at a gasoline pump). Also in some embodiments, a fixed base station may be connected to a desktop PC or a standalone base station and can be used for charging the intelligent electronic device and key. The base station may also be used to retrieve

financial card information for the desktop PC from the intelligent electronic device for electronic transactions. The transaction will occur only if both the intelligent electronic device and key are present. The fixed base station may also be used to include the optional magnetic card reader to initially download the information into the intelligent electronic device. In some embodiments, an organic light emitting diode (LED) display and flexible printed circuit board (PCB) may be used to design an intelligent electronic device that has the form factor and mechanical flexibility of a plastic card so that it can be carried inside a wallet. The intelligent electronic device may also act as an agent that holds other secure information such as user ID and password for access by the user after two or three factor authentications. Further, an intelligent electronic device that is enabled with wireless may be used to show on-demand advertisement and coupons on its display. The information displayed can depend on the card holder's usage pattern, if available.

For card-not-present on-line transactions, the mode of operation may be one of the following: (a) base station will verify the presence of the intelligent electronic device along with two or three factor authentication, explained above, or (b) if random or one-time use numbers are used, then with two or three factor authentication the intelligent electronic device will provide the correct number to use for card-not-present transactions similar to card present transactions.

In electronically programmable embodiments, the user does not have to deal with a third component, the generic card, unlike the magnetic card options described above. Further, the erasing of the information stored in the electronic stripe may be automatic, whereas in the magnetic card embodiments, erasing may depend on the user sliding the generic card back into the intelligent electronic device.

Note that the need for having access to the intelligent electronic device along with fingerprint scanning and the presence of the key provides a three-factor authentication. The same can be implemented without the key in which case the security of the information stored in the intelligent electronic device is achieved with two-factor authentication through fingerprint scanning. The key can also be replaced with a PIN input + fingerprint scanning to result in three-factor authentication. However, without the key the decryption code is

physically stored in the same device as that of the information and therefore susceptible to theft by hacking. The key along with the intelligent electronic device may be used as two-factor authentication.

Although the various embodiments of the present invention are described above using an intelligent electronic device and key, other devices may be utilized. For example, an intelligent electronic device may be a self powered smart card device that includes a display, fingerprint reader, and Bluetooth. Further, PIN entry or other biometric authentication can be used instead of fingerprint authentication.

Smart cards

Embodiments that include smart cards are now described with reference to Figures 1-6. Various embodiments of the present invention include: (i) an electronic device such as a personal digital assistant or an intelligent electronic device with smart card interface and wireless link such as Bluetooth; (ii) an electronic device such as a key that has memory and wireless link such as Bluetooth; (iii) the ability to generate predefined card numbers at random that will expire at the end of every transaction to eliminate card cloning and counterfeiting operations; and (iv) an empty generic smart card that can be programmed by the intelligent electronic device. The assumption here is that the point-of-sale uses smart cards.

The usage model is similar to that described above with reference to magnetic stripe cards, except the Intelligent Electronic Device programs the smart card instead of the magnetic stripe card.

In some embodiments, the intelligent electronic device and the smart card may be integrated into one device. This will result in a device similar to devices described above with reference to electronically programmed cards, except it is to be used for smart card point-of-sale.

Further, in some embodiments, a standalone smart card may be utilized without the intelligent electronic device. Each smart card will have an associated key. The smart card point-of-sale will verify if the associated key is present before approving the transaction. One feature of these embodiments is

that the smart card is not programmable to act as one of several cards and will require change in the point-of-sale.

Although the various embodiments of the present invention are described above using an intelligent electronic device and key, other devices may be utilized. Further, PIN entry or other biometric authentication can be used instead of fingerprint authentication.

Various embodiments described thus far include "programmable" financial cards, where "programmable" refers to the fact that the information for the card's stripe is programmable to represent one of several cards held by the card holder. Embodiments are now described that are applicable to authentication for bank checks.

Authentication for bank checks

Figure 7 shows an intelligent electronic device capable of printing checks. Intelligent electronic device 700 includes storage 744 for "blank" paper checks without account information, a wireless interface to support a wireless link 732 such as Bluetooth, a fingerprint scanner 712, a display screen 710, account selection and function buttons 708, and a miniature printer 742 to print checks. Also shown in Figure 7 is a key 730 that has memory and a wireless link such as Bluetooth.

The intelligent electronic device 700 will be preprogrammed with relevant account (or accounts) information including account holder name, mailing address, account number, and bank routing number. When the user is ready to use the check book s/he will power up the intelligent electronic device. The device will authenticate the user by verifying the presence of the key and/or fingerprint ID. Once authenticated, the user will pick the account of choice and optionally enter memo along with the transaction amount information. The printer then will print the account and transaction information on the blank paper check to produce a printed check 740. Any features discussed above with reference to programmable card embodiments may utilized with intelligent electronic device 700 without departing from the scope of the present invention. Further, PIN entry or other biometric authentication can be used instead of fingerprint authentication.

Financial Card Transaction Verification

Figures 8-10 show various methods for financial card transaction verification in accordance with various embodiments of the present invention. Figure 8 shows an example of "real time push verification," Figure 9 shows an example of "offline push verification," and Figure 10 shows an example of "offline pull verification." The embodiments represented by Figures 8-10 are applicable for all programmable financial card embodiments described herein and for all other standard cards.

When a transaction is initiated from the point-of-sale, credit card and transaction information is transferred to an acquirer 802 and a card issuing bank 804. These transfers are shown at 812 and 822 in Figures 8-10. The card issuing bank 804 transfers an approval or denial of the transaction to the acquirer 802 and ultimately to the point-of-sale. The transfers are shown at 824 and 814 in Figures 8-10. The acquirer 802 typically pays the merchant after verification. The card issuing bank 804 then pays the acquirer 802.

In various embodiments of the invention, an additional step is added either during information processing at the acquirer or at the card issuing bank. This additional step involves instant messaging to the card holder's phone/email with the necessary transaction details, which then when approved by the card holder is recorded to be a legitimate transaction. The phone 806 can be a mobile phone running special software that indicates to the user that a new transaction has arrived for approval. If the approval is not completed within a prescribed time the transaction is marked as a possible suspect and further defensive actions can be taken. The transaction records on the mobile device 806 can be downloaded onto PC financial software for record keeping. This transfer is shown at 840. Access to mobile device instant messaging can be restricted via PIN entry, voice recognition, or other biometric authentication such as fingerprint.

Figure 8 shows a real time push verification where the issuing bank 804 sends a real time message 832 to the mobile device 806 and waits for approval or denial at 834 before approving the transaction at 824. Figure 9 shows an offline push verification where the issuing bank 804 sends a message 832, but does not

wait for real time approval. Instead, a user may provide later notification of approval or denial at 934, and if necessary, the issuing bank 804 may take defensive action.

In other embodiments, instead of the information being pushed via automated mobile phone instant message, it can be an information pull based implementation, such as that shown in Figure 10. In information pull implementations, the transaction details are logged on a secure web site 1008 where the user visits periodically to approve the transactions at 1034.

Figure 11 show a flexible form factor for a programmable financial card. Programmable financial card 1100 has a flexible printed circuit board (PCB) that may include embedded integrated circuit components such as memory, processing, display driver, and wireless front end. In addition, programmable financial card 1100 may include a fingerprint reader, input buttons, organic LED display, and flexible battery power.

Figure 12 shows a perspective exploded view of the programmable financial card of Figure 11. Programmable financial card 1100 includes flexible PCB 1202, programmable stripe 1204, organic LED display 1216, and fingerprint input device 1214. Flexible PCB 1202 includes flexible battery 1208, battery charging by contactless coupling 1206, memory, processing, and display driver integrated circuits 1210, and wireless front end integrated circuit and antenna 1212.

Figure 13 shows usage models for a secondary wireless device in card-present transactions and card-not-present transactions. Usage models for card-not-present transactions are show in the top portion of Figure 13, shown generally at 1302. In these embodiments, secondary wireless device 1310 communicates with various types of electronic devices that in turn communicate with point-of-sale terminals or merchants without a reprogrammable card present. For example, secondary wireless device 1310 may provide user transparent automated authentication with a home computer and base station 1320, laptop computer 1330, personal digital assistant (PDA) 1340, or cellular telephone 1350. These devices may then in turn communicate with merchants using one or more secure protocols such as: Secure Electronic Transaction

(SET), Mobile electronic Transaction (MeT); M-payments; or other emerging standards.

Usage models for card-present transactions are show in the bottom portion of Figure 13, shown generally at 1304. In these embodiments, secondary wireless device 1310 provides user transparent automated authentication with one or more of a reprogrammable card 1360 and portable transaction device 1370. Reprogrammable card 1360 may then communicate with point-of-sale terminals or merchants.

Multi-factor authentication may be utilized in both card-present and card-not-present transactions. For example, two factor or three factor authentication may be provided as described above with reference to Figures 1-6.

Figure 14 shows an architecture diagram for a transaction system with multi-factor authentication. Architecture 1400 is a layered architecture that represents any of the transaction systems described herein. For example, architecture 1400 may represent a portable transaction device in combination with a programmable stripe or a reprogrammable card such as those shown in Figures 1 and 2.

Architecture 1400 includes an application layer 1410, a first virtual layer 1420, a standards layer 1430, a second virtual layer 1440, and a physical layer 1450. Architecture 1400 may include more layers than those shown in Figure 14, and further, no layer shown is meant to be essential.

Application layer 1410 includes original equipment manufacturer (OEM) software (SW) 1412 and value added software 1414. OEM SW 1412 may include any software provided by a manufacturer of a portable transaction device. For example, OEM SW 1412 may include a phone book, contacts, and other software. Value added SW 1414 may include any software that directly or indirectly supports the transaction system. For example, value added SW 1414 may include a graphical user interface (GUI) for card information download, authentication, card selection, voice component, single use account number generation, e-wallet applications, or the like. Value added SW 1414 may also include a voice recognition component to record transactions for download to money management software. The foregoing list is not meant to be exhaustive, and no portion of the list is meant to be essential.

Virtual layer 1420 provides an application programming interface (API). The API in virtual layer 1420 may be provided by an OEM, or by a value added business, or both. For example, an OEM API may provide an interface for third party developers to develop applications for the portable transaction device. Also for example, a value added API may provide an interface for third party developers to develop applications for the combination of portable transaction device and programmable stripe or reprogrammable card.

Standards layer 1430 provides operation in compliance with one or more standards. As shown in Figure 14, standards layer 1430 provides operation in compliance with at least multimedia and communications standards. Example standards include, but are not limited to: telephony standards, TCP/IP, GPRS, USB, Bluetooth, IrDA, SMS, MMS, ECML, SSL, TLS, JPEG, MPEG, and MP3.

Virtual layer 1440 includes operating system (OS) and device drivers. Example operating systems include, but are not limited to: Symbian, Microsoft Mobile, PalmOS, and Linux. Device drivers may include drivers to provide an interface to hardware in physical layer 1450.

Physical layer 1450 includes OEM hardware 1452 and value added hardware 1454. OEM hardware 1452 may include any hardware provided by a manufacturer. For example, in embodiments where the portable transaction device is a mobile phone, OEM hardware 1452 includes the phone and any accessories provided by the OEM. Value added hardware 1454 may a reprogrammable card or stripe. In some embodiments the card or stripe may be tightly coupled to the OEM hardware and in other embodiments, the card or stripe may be insertable and removable. Physical layer 1450 may also include a voice component, image component, fingerprint capture component, a link to a secondary wireless device, or the like.

Figure 15 shows usage models for electronic money transfer. The usage model shown in Figure 15 represents the electronic transfer of money from portable transaction device 1 (1504) to portable transaction device 2 (1524). Portable transaction device 2 is also shown at 1550 ready to perform a transaction after authentication.

Money may be transferred electronically from portable transaction device 1 may be under a new debit card account or other account. Portable transaction device 1 requests a transfer from bank 1502 at 1503, and portable transaction device 2 may receive the electronic transfer either directly from portable transaction device 1 at 1507 or through a mobile network at 1513. For example, a direct transfer at 1507 may include communications via Infrared (IrDA), Bluetooth, cabling, or other interface. Also for example, a transfer using a mobile network may include portable transaction device 2 communicating over a data network at 1513 to receive the electronic transfer.

After the transfer, portable transaction device 2 may be used in a financial transaction. For example, a user may authenticate, shown generally at 1540, and then portable transaction device 2 may be used at 1550. A user may authenticate using any type of single or multi-factor authentication described herein. After authentication, device 1550 may be used in a financial transaction such as a merchant transaction at a point-of-sale, an ATM machine, or another transfer into a different account.

The transaction may be a card-present or card-not-present transaction. For example, a card present transaction may be performed using stripe 1560, and a card-not-present transaction may be performed using a card number that represents the account to which the money has been transferred. The card number may be a static number or may be a one time use number.

Figure 16 shows usage models for pre-paid card recharge. The usage model shown in Figure 16 represents the recharge of a stored value card or pre-paid card. For example, the holder of portable transaction device 1 may authorize a pre-paid card increase at 1634, and bank 1602 may increase the value of a pre-paid card at 1636. Portable transaction devices 1 and 2 may communicate either directly or indirectly through a mobile network at 1607. Communications 1607 may include portable electronic device 2 requesting an increase in value, and portable transaction device 1 either granting or denying a change in value.

When portable transaction device 2 receives an increase in value of a stored value or pre-paid card, and a user has authenticated, a card-present or card-not-present transaction may be performed as described above.

Figure 17 shows business methods. Business 1710 is a business that profits from use of the transactions systems described herein. Figure 17 is shown in the context of cellular phones being used as portable transaction devices in the transaction systems described herein, but this is not a limitation of the present invention. For example, other business methods utilize personal digital assistants (PDAs) or handheld computers as portable transaction devices.

Business 1710 may or may not manufacture value added hardware such as devices having programmable stripes, and may or may not produce value added software. In some embodiments, business 1710 owns intellectual property relating to value added hardware and software, and licenses that intellectual property. In other embodiments, business 1710 also produces value added hardware and/or software, and income is derived from those activities.

As shown in Figure 17, business 1710 may receive fees from many potential sources, including card-issuing banks 1720, phone manufacturers 1730, phone service operators 1740, customers, and third parties.

The following numbered paragraphs provide further disclosure of the systems and methods of the present description:

1. A financial transaction authentication system, including a mobile telephone (or handheld computer or other portable electronic device) having a biometric scanner and a transaction stripe that may be operatively engaged with a point-of-sale stripe reader, where the financial transaction authentication system is configured to combine biometric information with one or more additional authentication factors to secure financial transactions.

2. The system of paragraph 1, where the stripe is attached to the mobile telephone.

3. The system of paragraph 1, where the stripe is provided on a separate structure (e.g., a structure shaped and sized like a traditional financial card) that may be selectively inserted into and removed from the mobile telephone.

4. The system of paragraph 1, further comprising software configured to control financial transaction communication between the mobile telephone and various external systems involved in financial transaction, and

configured to control communications between the mobile telephone and access controls implemented in buildings, cars etc.

5. The system of paragraph 1, further comprising software configured to implement and apply one-time use numbers on to the transaction stripe, wherein this may include local generation of the one-time use numbers or download of one-time use numbers via a mobile telephone network.

6. The system of paragraph 1, where the information is encoded onto the transaction stripe via electrical voltage pulses that generate magnetic fields to mimic magnetic stripe tracks in standard financial transaction cards. The sequence of pulses of time duration T and 2T may be used to code for 1 and 0. Since the pulse train is not stored magnetically the stripe length can be much smaller than that of a standard card. The card substrate can thus be much smaller than a traditional financial card. The card may include the transaction stripe, optional memory and optional energy storage to support complete detaching from the mobile telephone. The detachable card may also include wireless capability to communicate to the mobile telephone.

7. The system of paragraph 1, where in multi-factor authentication, biometric data (e.g., fingerprint) is used to access the mobile phone device and PIN entry is required to access account information.

8. The system of paragraph 1, further comprising a secondary wireless device, such as a key fob, that is used to provide an additional authentication factor, namely that the mobile telephone will not allow access to the financial card account information unless the secondary wireless device is in the vicinity. Wireless key can be implemented via bluetooth protocol as an example.

9. The system of paragraph 1, where the mobile telephone is employed as a wireless authentication key for two factor authentication in accessing other electronic systems such as laptops, PCs, cars etc.

10. The system of paragraph 1, where the mobile telephone is used for card consolidation, in that information for multiple accounts is stored within a memory in the mobile telephone, and where the user may select a particular account and after proper authentication, the account information for the selected account is applied to the transaction stripe.

11. The system of paragraph 1, where since the system may be configured to require two or more factor authentication for gaining access to account information, the system may be employed for secure card present and card not present transactions. Also, since the one-time use number generation is integrated into the mobile telephone, card present or card not present solutions can take advantage of this security feature.

12. The system of paragraph 1, where since the information on the electronic stripe is not coded in physical locations on the magnetic stripe more bits can be conveyed to the POS between the start and the stop sentinels. These additional bits can be used to have unique ID independent of any account information. This will ensure that even if account information is stolen without this unique ID in the stripe the transaction will not be valid. So a cloned card based on known account information will not make the transaction valid without this unique ID.

13. The system of paragraph 1, where since the mobile telephone device is connected to a mobile phone network, the account holder can set a per-transaction amount limit and if a transaction exceeds that limit the user will receive a secure SMS message (or a message via any other mobile network-based messaging service) requesting validation of the transaction; the transaction will be authenticated only after the user replies the SMS with an 'overlimit' password; the password will be independent of other passwords. Note that the per-transaction limit could be zero, which will require secure SMS authentication every transaction; also, if the mobile phone is not in a cell then the financial card issuing bank will note it as a 'risky' transaction and take appropriate action, such as invalidate the account for future transaction.

14. The system of paragraph 1, where since the mobile telephone device is connected to the mobile phone network, the account activation may happen via the mobile network after 2- or 3-factor authentication. Authentication may also happen via the mobile phone network; for example, a user will have to make a phone call and the system will verify the user's voice; once the voiceprint is verified, the mobile network will be used to download the financial card information onto the mobile telephone device.

15. The system of paragraph 1, where the mobile telephone device will also use the voice recording component in the mobile phones to record user voice keywords. The keywords will include the type of transaction and the amount of transaction. The keywords can then be downloaded into a PC with voice recognition for automated data entry into software such as Microsoft Money or Quicken. The mobile telephone device can have two directional microphones, one for recording background noise and one for recording voice and background noise. This will improve voice recognition by canceling out background noise.

16. The system of paragraph 1, where the mobile phone network can also be used to upload account summary automatically from the card issuing bank. This can then be downloaded into a PC. All connections to the PC will be via an optional base station. The base station will also be used to charge the phone.

17. The system of paragraph 1, where the mobile phone network can also be used to update the cell phone service provider of the financial transaction details. This can be used to consolidate the mobile phone bill with the credit card transaction bill.

18. The system of paragraph 1, where since the mobile telephone device is connected to the mobile phone network, if the device is stolen the mobile phone network can be used to call the phone to delete all account information. Also, the network can be used to track a delinquent account holder.

19. The system of paragraph 1, where since the mobile telephone device is connected to the mobile phone network, gift cards and other stored value cards can be directly transmitted to a recipient if his/her telephone number is known.

20. The system of paragraph 1, where the mobile phone network can be used to upload user-specific ads/coupons into the mobile telephone device. This can also involve using Bluetooth or Infrared network to upload user specific ads/coupons.

21. The system of paragraph 1, where messages sent via the mobile phone network to and from the mobile telephone will be encrypted. Each mobile

telephone device will have a unique private and public key which will be used for sending secure information.

22. The system of paragraph 1, where since the mobile telephone device provides secure storage of information, it can be extended to store not such financial data but also other user information such as login IDs and passwords, account numbers for building access, user ID for access to cars, etc.

23. The system of paragraph 1, where the portable electronic device is configured to take photographs, and where a photograph of a user is taken during initial activation, and where such photograph is later employed to increase the security of a financial transaction (e.g., by providing an additional authentication factor).

24. The system of paragraph 1, where the portable electronic device is voice-activated.

25. The system of paragraph 1, where the transaction stripe is magnetically encoded via a magnetic head of the portable electronic device.

26. The system of paragraph 1, where the system is implemented using open technologies and specifications, such as ECML (electronic commerce modeling language).

27. The system of paragraph 1, where communications are secured via secure protocols such as TLS and SSL.

28. The system of paragraph 1, where the mobile telephone (or other electronic device) may be operatively interfaced with another such device to perform a peer-to-peer value transfer.

29. The system of paragraph 1, where the system may be employed to refresh value in a stored value card or like device.

30. The system of paragraph 29, where the stored value is refreshed via a mobile telephone network.

31. The system of paragraph 1, where financial card information is stored in a SIM device associated with and operatively engaged with the mobile telephone.

Although the present invention has been described in conjunction with certain embodiments, it is to be understood that modifications and variations may be resorted to without departing from the spirit and scope of the invention

as those skilled in the art readily understand. Such modifications and variations are considered to be within the scope of the invention and the appended claims.

IPR2025-00644 Page 01116

What is claimed is:

1. A portable transaction device comprising:
memory to hold information regarding a financial card;
a slot to interface with a reprogrammable card; and
software to generate single use transaction numbers.

2. The portable transaction device of claim 1 further comprising a biometric scanner where the portable transaction device is configured to combine biometric information with one or more additional authentication factors to secure financial transactions.

3. The portable transaction device of claim 1 further comprising a wireless interface to communicate with a secondary wireless device for an additional authentication factor.

4. The portable transaction device of claim 1 further comprising controls to allow a user to select one of a plurality of financial cards with which to program the transaction stripe.

5. A portable transaction device comprising:
means for interacting with a user to provide a first authentication factor;
means for interacting with a secondary wireless device to provide a second authentication factor; and
software to request a change in value of a pre-paid card.

6. The portable transaction device of claim 5 wherein the means for interacting with a user comprises a biometric input device.

7. The portable transaction device of claim 6 wherein the biometric input device comprises a fingerprint scanner.

IPR2025-00644 Page 01117

8. The portable transaction device of claim 5 wherein the portable transaction device comprises a cellular phone.

9. The portable transaction device of claim 8 wherein the software to request a change in the value of a pre-paid card comprises software on the cellular phone to communicate with a mobile network.

10. The portable transaction device of claim 8 wherein the software to request a change in the value of a pre-paid card comprises software on the cellular phone to communicate with another portable transaction device.

11. The portable transaction device of claim 5 further comprising a slot to receive the pre-paid card.

12. A portable transaction device comprising:

a user authentication component to allow a user to authenticate to the portable transaction device;

a cellular telephone component; and

a value transfer component to operatively interface to another portable transaction device to refresh value in a stored value card.

13. The portable transaction device of claim 12 wherein the value transfer component operatively interfaces with another portable transaction device using the cellular telephone component.

14. The portable transaction device of claim 12 wherein the value transfer component operatively interfaces with another portable transaction device using an Infra-red signal.

15. The portable transaction device of claim 12 wherein the user authentication component includes a biometric input device.

16. The portable transaction device of claim 15 wherein the user

IPR2025-00644 Page 01118

authentication component further includes a wireless interface to communicate with a secondary wireless device.

17. A financial transaction system comprising:

a reprogrammable financial card; and

a cellular telephone having an interface to communicate with the reprogrammable card, wherein the cellular telephone includes a software component to request a change in value of a financial account.

18. The financial transaction system of claim 17 wherein the financial account represents a stored value card, and the reprogrammable card may be programmed to operate as the stored value card.

19. the financial transaction system of claim 17 wherein the financial account is accessible using a debit card, and the reprogrammable card may be programmed to operate as the debit card.

20. The financial transaction system of claim 17 further comprising a wireless interface to communicate with a secondary wireless device for authentication.

IPR2025-00644 Page 01119

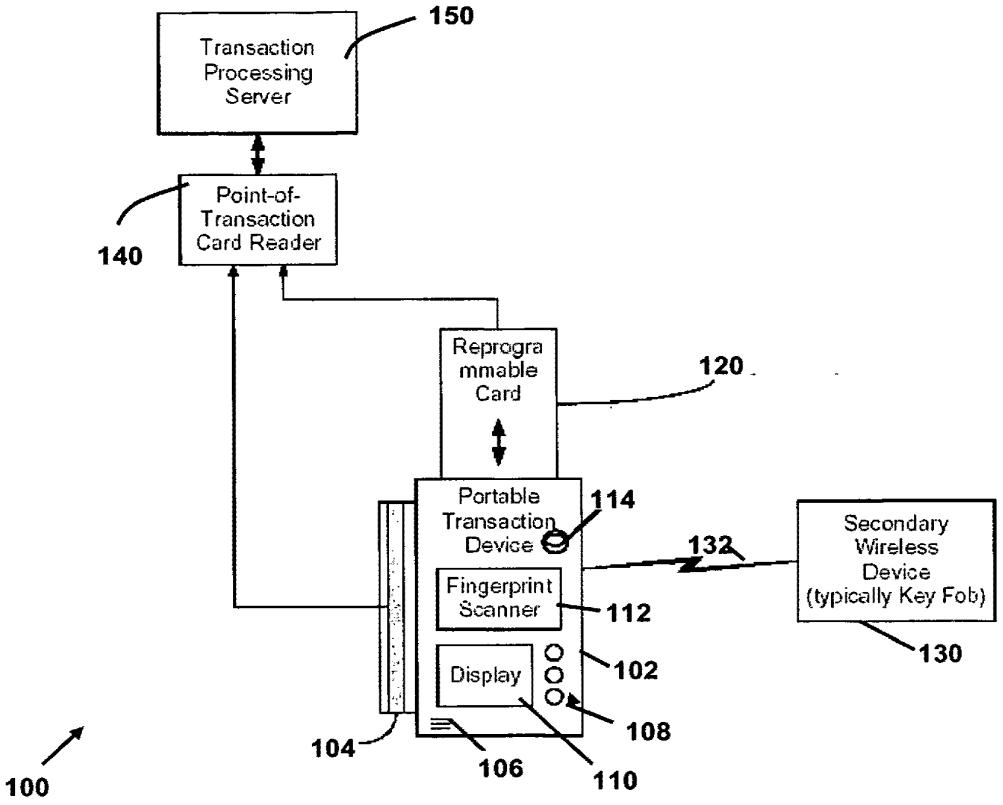

Transaction Processing Server
150
Point-of-Transaction Card Reader
140
Reprogra mmable Card
120
Portable Transaction Device
114
Fingerprint Scanner
112
Display
102
108
Secondary Wireless Device (typically Key Fob)
132
130
104
106
110
100

Fig. 1

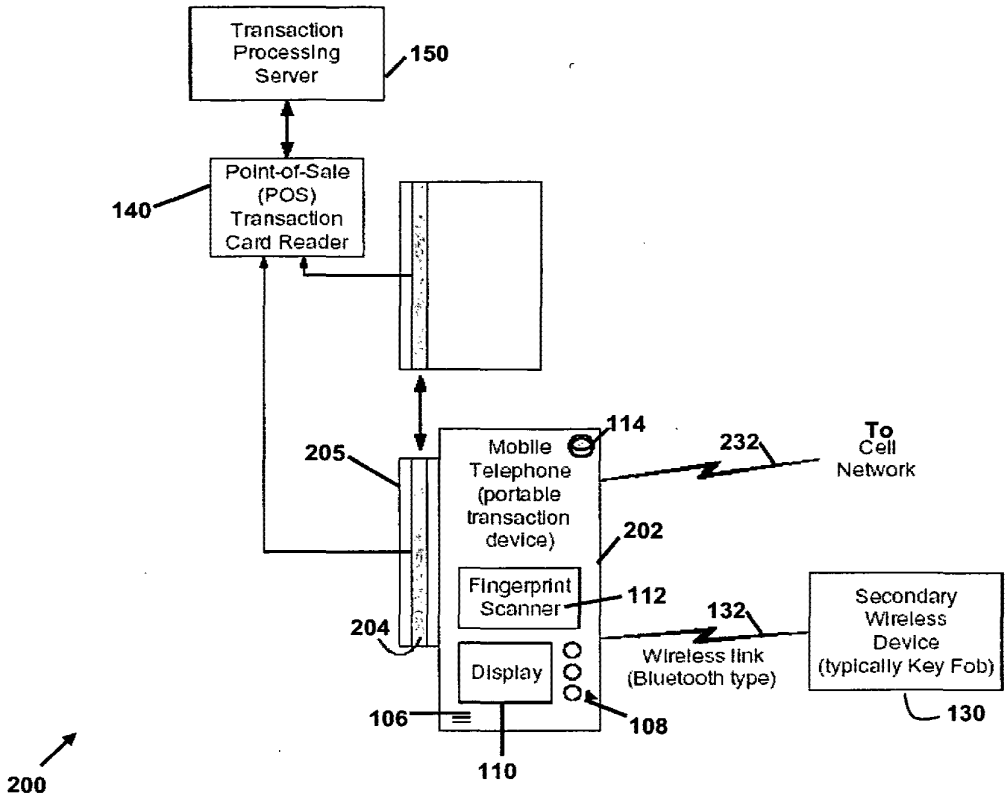

Transaction Processing Server
150
Point-of-Sale (POS) Transaction Card Reader
140
205
Mobile Telephone (portable transaction device)
114
232
To Cell Network
202
Fingerprint Scanner
112
132
Secondary Wireless Device (typically Key Fob)
130
204
Display
Wireless link (Bluetooth type)
106
108
110
200

Fig. 2

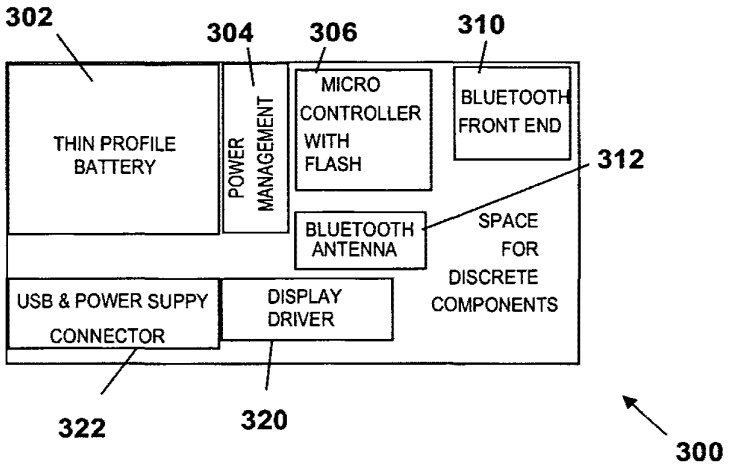

302
304
306
310
THIN PROFILE BATTERY
POWER MANAGEMENT
MICRO CONTROLLER WITH FLASH
BLUETOOTH FRONT END
312
BLUETOOTH ANTENNA
SPACE FOR DISCRETE COMPONENTS
USB & POWER SUPPY CONNECTOR
DISPLAY DRIVER
322
320
300

Fig. 3

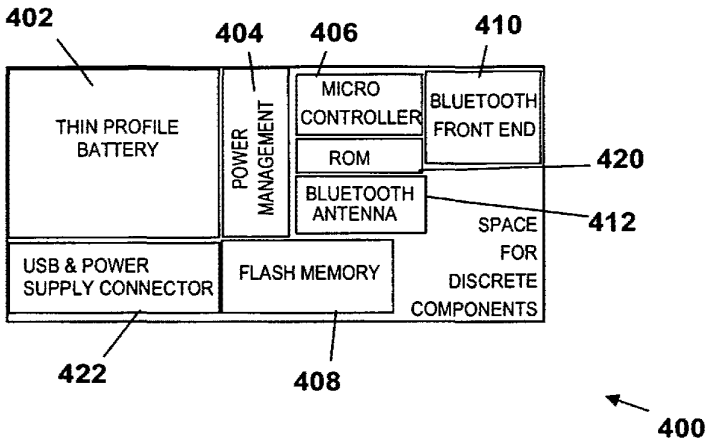

402
404
406
410
THIN PROFILE BATTERY
POWER MANAGEMENT
MICRO CONTROLLER
BLUETOOTH FRONT END
ROM
420
BLUETOOTH ANTENNA
412
SPACE FOR DISCRETE COMPONENTS
USB & POWER SUPPLY CONNECTOR
FLASH MEMORY
422
408
400

Fig. 4

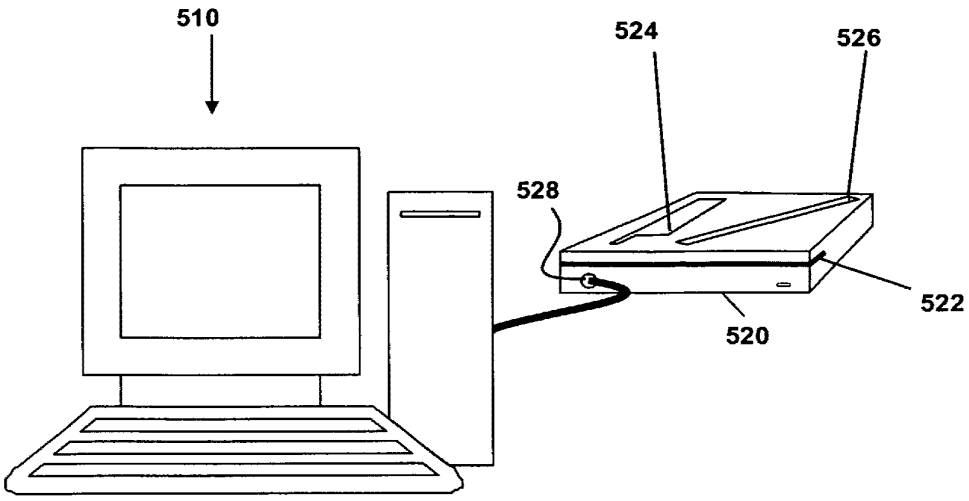


Fig. 5

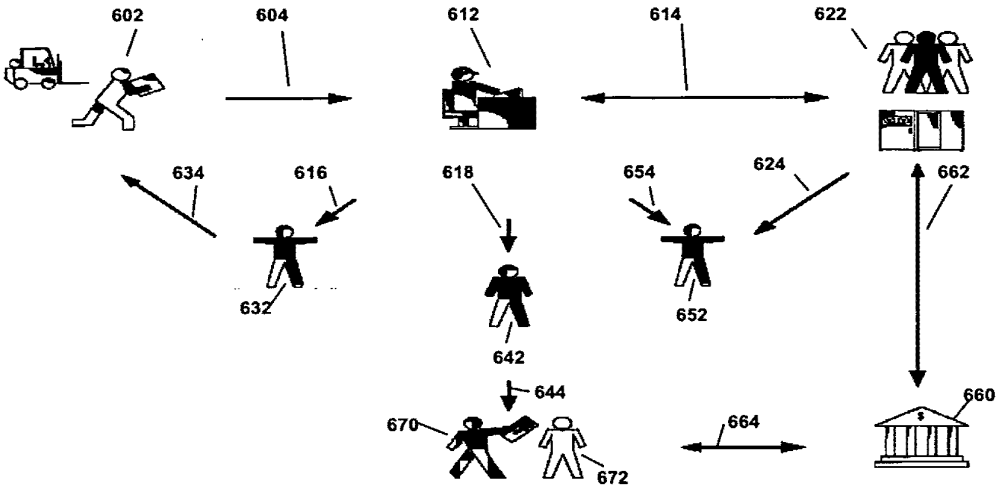

602
604
612
614
622
634
616
618
654
624
662
632
642
652
644
660
670
664
672

Fig. 6

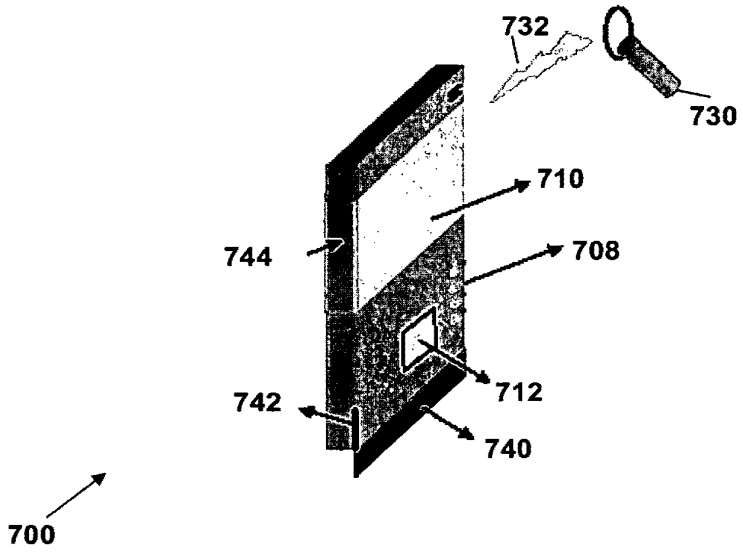


Fig. 7

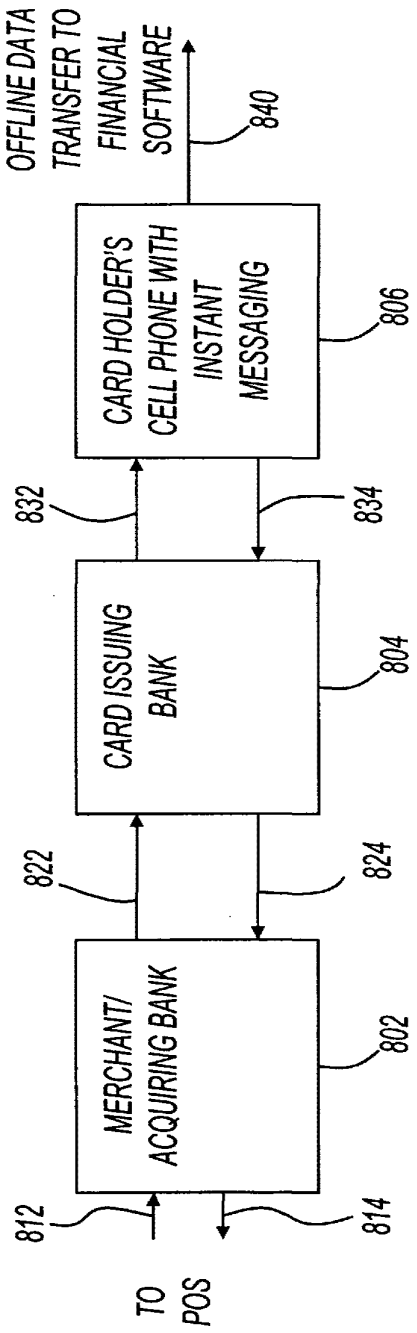

OFFLINE DATA TRANSFER TO FINANCIAL SOFTWARE
840
CARD HOLDER'S CELL PHONE WITH INSTANT MESSAGING
806
832
834
CARD ISSUING BANK
804
822
824
MERCHANT/ ACQUIRING BANK
802
812
814
TO POS

FIG. 8

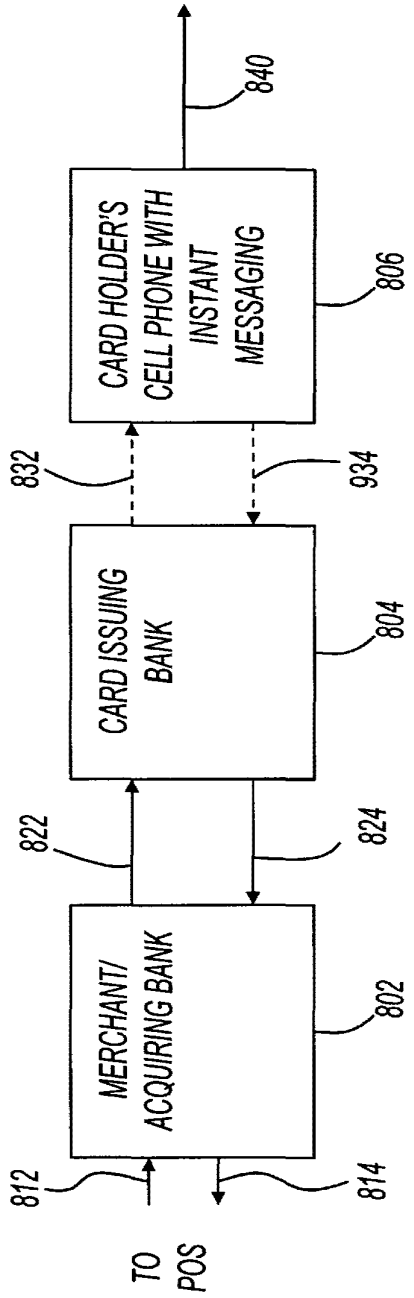

840
CARD HOLDER'S CELL PHONE WITH INSTANT MESSAGING
806
832
934
CARD ISSUING BANK
804
822
824
MERCHANT/ ACQUIRING BANK
802
812
814
TO POS

FIG. 9

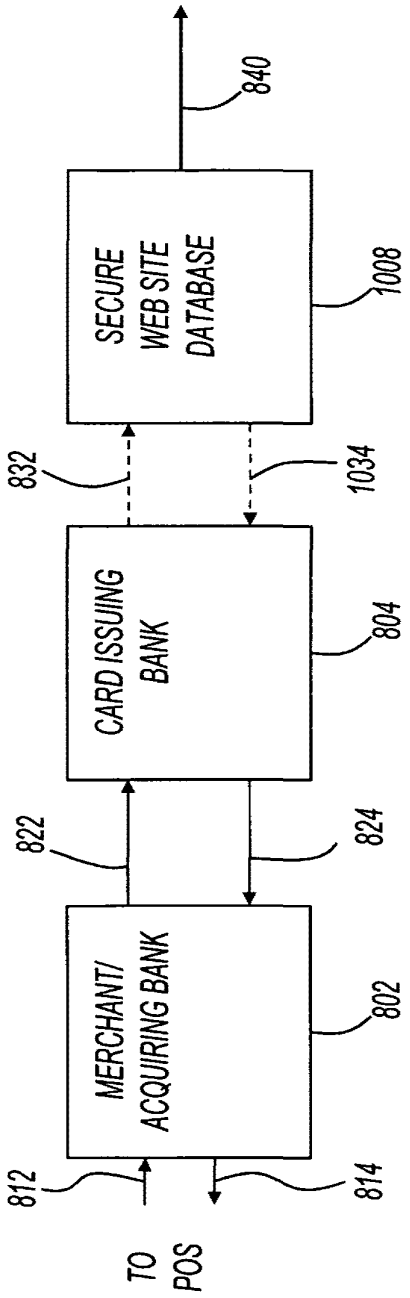

840
SECURE WEB SITE DATABASE
1008
832
1034
CARD ISSUING BANK
804
822
824
MERCHANT/ ACQUIRING BANK
802
812
814
TO POS

FIG. 10

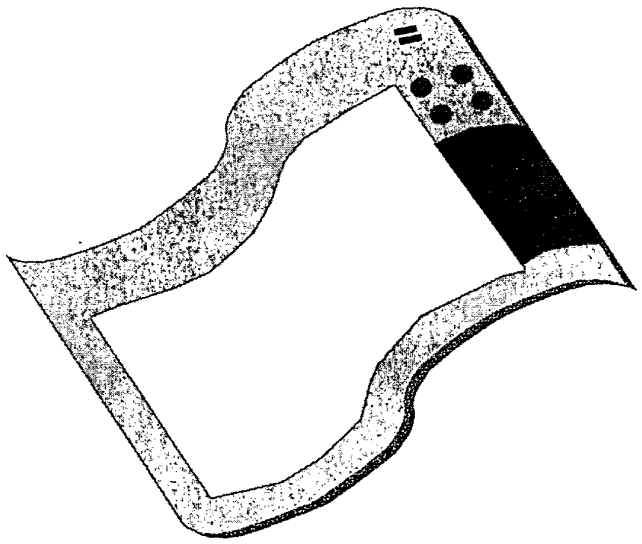


Fig. 11

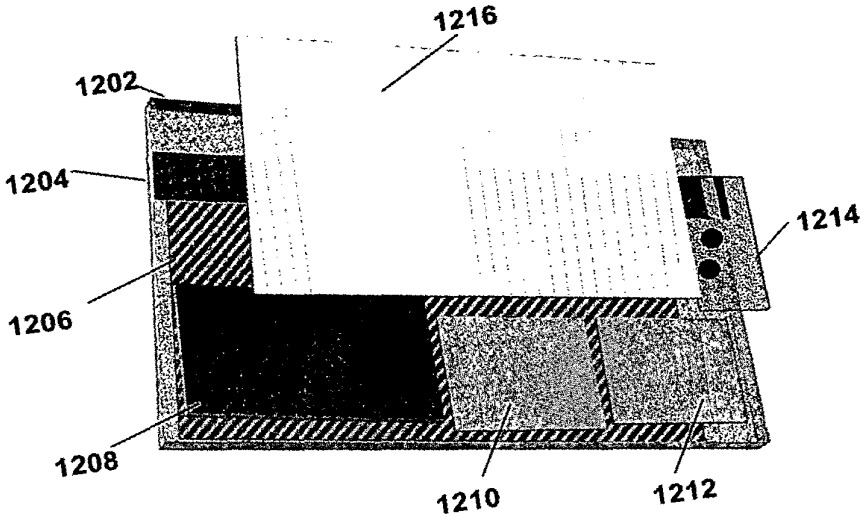


Fig. 12

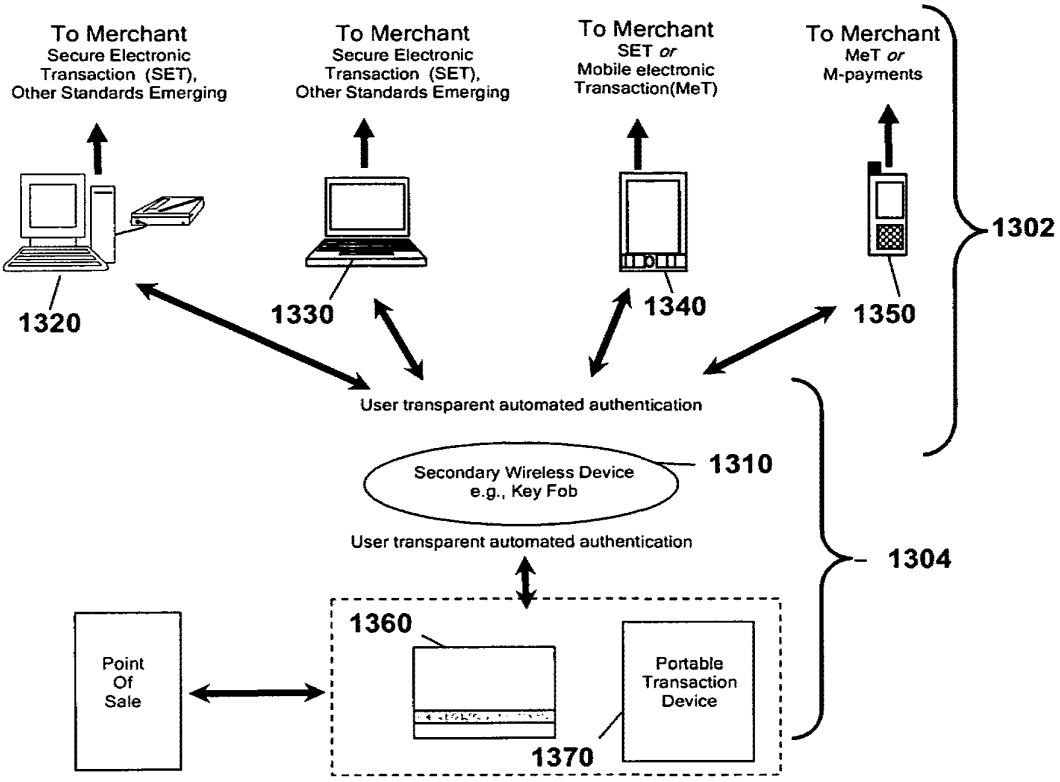

To Merchant
Secure Electronic Transaction (SET), Other Standards Emerging
To Merchant
Secure Electronic Transaction (SET), Other Standards Emerging
To Merchant
SET or Mobile electronic Transaction(MeT)
To Merchant
MeT or M-payments
1320
1330
1340
1350
1302
User transparent automated authentication
Secondary Wireless Device e.g., Key Fob
1310
User transparent automated authentication
1304
1360
Point Of Sale
Portable Transaction Device
1370

Fig. 13

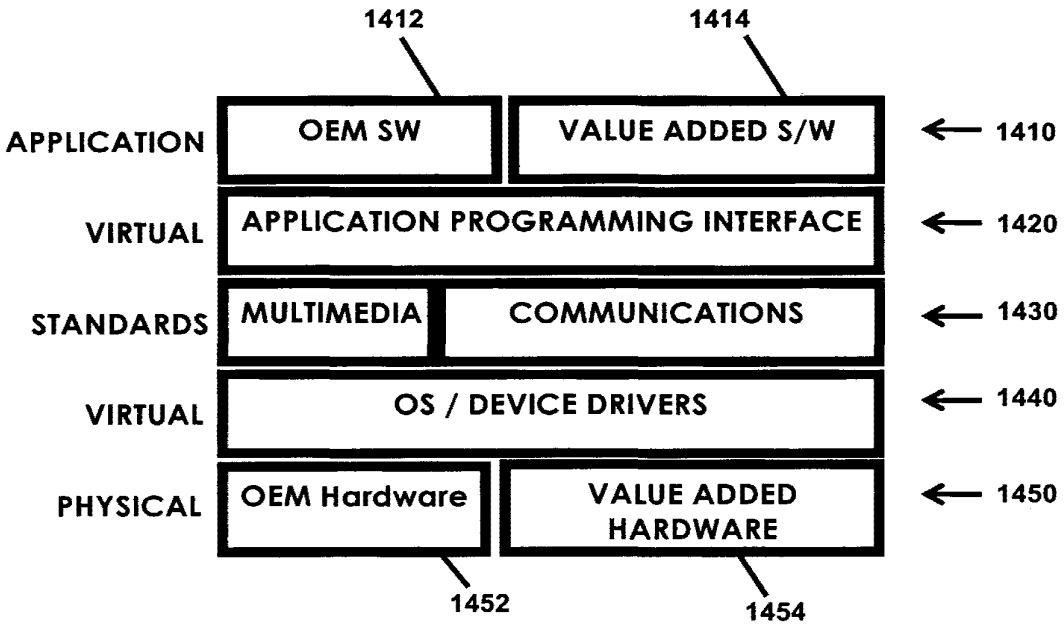

1412
1414
APPLICATION
OEM SW
VALUE ADDED S/W
1410
VIRTUAL
APPLICATION PROGRAMMING INTERFACE
1420
STANDARDS
MULTIMEDIA
COMMUNICATIONS
1430
VIRTUAL
OS / DEVICE DRIVERS
1440
PHYSICAL
OEM Hardware
VALUE ADDED HARDWARE
1450
1452
1454

Fig. 14

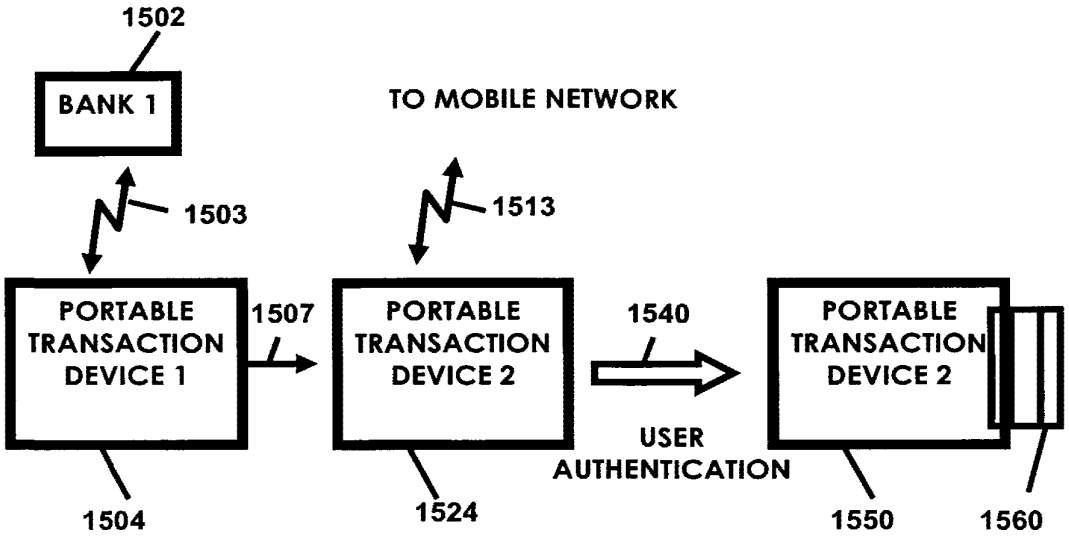

1502
BANK 1
TO MOBILE NETWORK
1503
1513
PORTABLE TRANSACTION DEVICE 1
1507
PORTABLE TRANSACTION DEVICE 2
1540
PORTABLE TRANSACTION DEVICE 2
USER AUTHENTICATION
1504
1524
1550
1560

Fig. 15

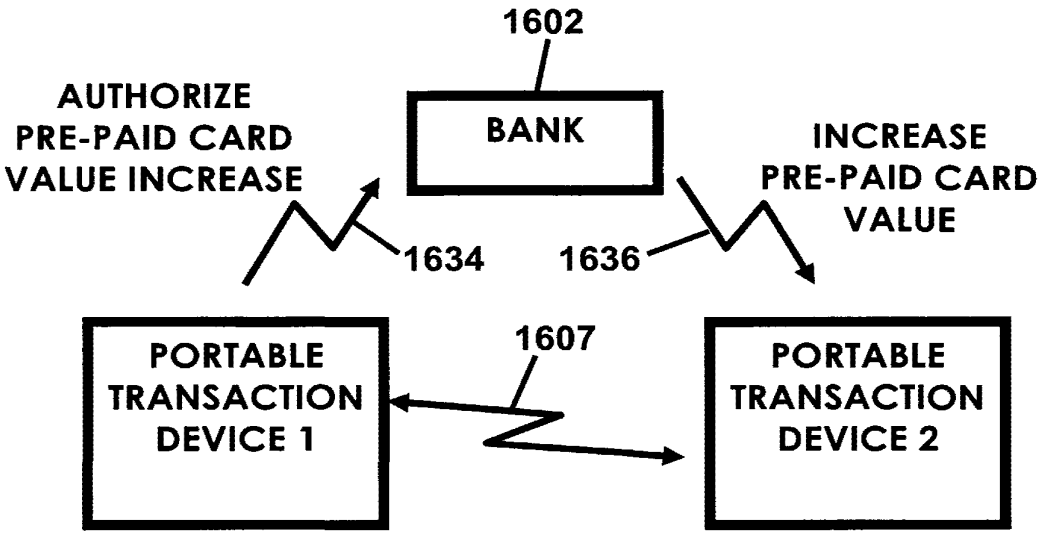

1602
BANK
AUTHORIZE
PRE-PAID CARD
VALUE INCREASE
INCREASE
PRE-PAID CARD
VALUE
1634
1636
1607
PORTABLE
TRANSACTION
DEVICE 1
PORTABLE
TRANSACTION
DEVICE 2

Fig. 16

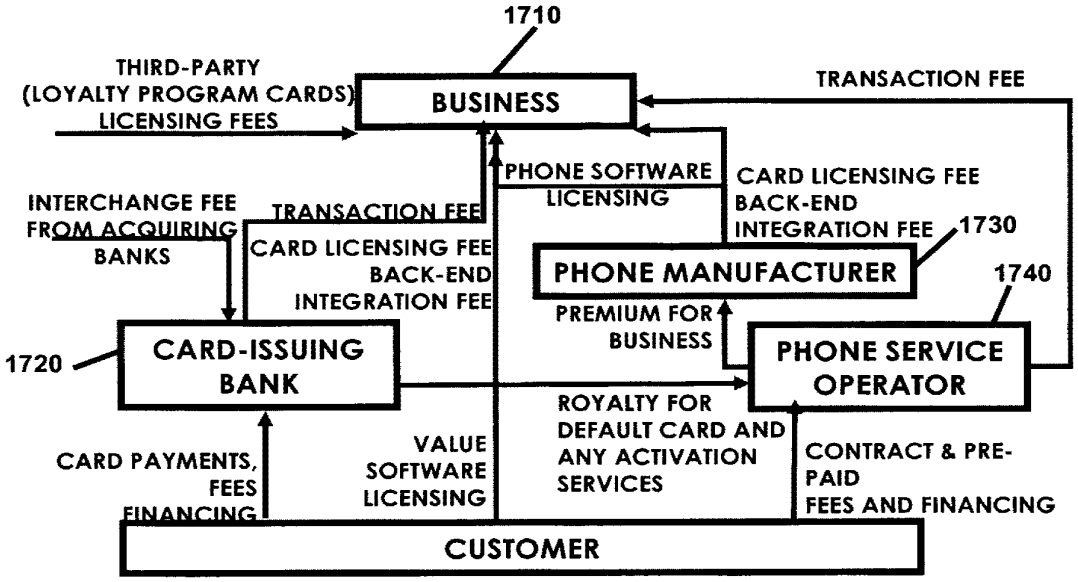

1710
THIRD-PARTY
(LOYALTY PROGRAM CARDS)
LICENSING FEES
BUSINESS
TRANSACTION FEE
PHONE SOFTWARE
LICENSING
CARD LICENSING FEE
BACK-END
INTEGRATION FEE
1730
INTERCHANGE FEE
FROM ACQUIRING
BANKS
TRANSACTION FEE
CARD LICENSING FEE
BACK-END
INTEGRATION FEE
PHONE MANUFACTURER
1740
PREMIUM FOR
BUSINESS
1720
CARD-ISSUING
BANK
PHONE SERVICE
OPERATOR
ROYALTY FOR
DEFAULT CARD AND
ANY ACTIVATION
SERVICES
CARD PAYMENTS,
FEES
FINANCING
VALUE
SOFTWARE
LICENSING
CONTRACT & PRE-
PAID
FEES AND FINANCING
CUSTOMER

Fig. 17

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 December 2005 (15.12.2005)

PCT

(10) International Publication Number
WO 2005/119608 A1

(51) International Patent Classification[7]: G07F 19/00, 7/10

(21) International Application Number:
PCT/US2005/022993

(22) International Filing Date: 3 June 2005 (03.06.2005)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/576,894 3 June 2004 (03.06.2004) US

(71) Applicant *(for all designated States except US)*: **TYFONE, INC.** [US/US]; 1490 Clifton Street, Portland, OR 97201 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **SPITZER, Thomas, N.** [US/US]; 1490 Clifton Street, Portland, OR 97201 (US). **TADEPALLI, Prabhakar** [US/IN]; 290 Phase II, Adarsh Palm Meadows, Airport Whitefield Road, Bangalore 560066, Karnataka (IN). **NARENDRA, Siva, G.** [IN/US]; 7180 SW 84th Avenue, Portland, OR 97223 (US).

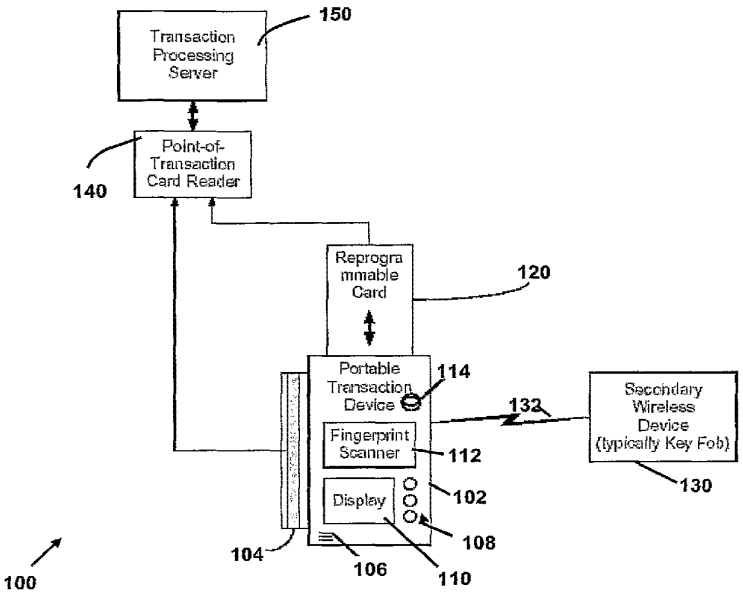
(74) Agent: **LEMOINE, Dana, B.**; LeMoine Patent Services, PLLC, c/o Portfolio IP, P.O. Box 52050, Minneapolis, MN 55402 (US).

(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, KE, KG, KM, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, 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, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, MC, NL, PL, PT, RO,

[Continued on next page]

(54) Title: SYSTEM AND METHOD FOR SECURING FINANCIAL TRANSACTIONS



(57) Abstract: A financial transaction system utilizes multi-factor authentication to secure financial transactions. The system comprises a portable transaction device (e.g. a wireless phone) which is used to program the magnetically or electronically reprogrammable stripe of a magnetic stripe card or the memory of a smart card. A single-use account number may be used to program the card. The device provides a biometric authentication and secondary authentication using a secondary wireless device.

WO 2005/119608 A1

SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, 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.

SYSTEM AND METHOD FOR SECURING FINANCIAL TRANSACTIONS

Field

The present invention relates generally to portable transaction devices, and more specifically to portable transaction devices having various security features.

Background

Instances of financial card fraud and identity theft have increased dramatically in recent years, particularly with the rapid increase of online and electronic transactions. Solutions of varying efficacy have been proposed to protect financial information and otherwise guard against fraud and theft. Firewalls protect computer systems against unauthorized access; however, they cannot be completely assured of the identities of individuals accessing the network. Various electronic devices may be employed to verify the identity of individuals; however, these devices often permit authentication information to be accessed. Some systems provide significantly improved security, but at the expense of requiring substantial changes to point-of-sale devices or other parts of the transactional infrastructure.

Brief Description of the Drawings

Figures 1 and 2 show transaction systems with multi-factor authentication;

Figure 3 shows a block diagram of a programmable card;

Figure 4 shows a block diagram of a secondary wireless device;

Figure 5 shows a computer and base station;

Figure 6 shows usage models for various embodiments of the present invention;

Figure 7 shows an intelligent electronic device capable of printing checks;

Figures 8-10 show various methods for financial card transaction verification in accordance with various embodiments of the present invention;

Figure 11 shows a flexible form factor for a programmable financial card;

Figure 12 shows an exploded perspective view of the programmable financial card of Figure 11; and

Figure 13 shows usage models for a secondary wireless device in card-present transactions and card-not-present transactions.

Description of Embodiments

In the following detailed description, reference is made to the accompanying drawings that show, by way of illustration, various embodiments of an invention. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention. It is to be understood that the various embodiments of the invention, although different, are not necessarily mutually exclusive. For example, a particular feature, structure, or characteristic described in connection with one embodiment may be implemented within other embodiments without departing from the spirit and scope of the invention. In addition, it is to be understood that the location or arrangement of individual elements within each disclosed embodiment may be modified without departing from the spirit and scope of the invention. The following detailed description is, therefore, not to be taken in a limiting sense, and the scope of the present invention is defined only by the appended claims, appropriately interpreted, along with the full range of equivalents to which the claims are entitled. In the drawings, like numerals refer to the same or similar functionality throughout the several views.

The present disclosure relates generally to use of a portable transaction device having various security features. The security features may be employed to particular advantage in financial transactions, so as to enhance security beyond that currently available in transactions conducted with financial cards, bank checks and existing computing devices. Traditionally, financial cards have information physically present on the front face and in the magnetic stripe. Similarly, bank account number, account holder's name, routing number and the address are present in the face of the checks. If a financial card or a checkbook is lost or stolen, or if the card is skimmed (an unauthorized swipe to gather card

holder information stored on the stripe), the information is insecure and is available for use by anyone. Similar risks are present with computing devices and other electronic devices used in financial transactions.

Accordingly, as shown in Fig. 1, a transaction system 100 with multi-factor authentication may be employed. As shown in this embodiment, the system 100 may include: a central transaction processing server 150; a point-of-sale transaction card reader 140; a portable transaction device 102 for use in credit/debit card type transactions; a key fob or other secondary wireless device 130 configured to wirelessly communicate with the portable transaction device 102; a reprogrammable card 120 that may be inserted into the portable transaction device 102 and reprogrammed with a one-time use transaction number or a reprogrammable electronic stripe 104 attached directly to the portable transaction device 102.

The portable transaction device 102 may include a camera (video and picture) component 114, a biometric (e.g., fingerprint) scanner 112, a display 110, a voice (microphone and speaker) component 106, and controls 108. The portable transaction device 102 may also include voice-activation and camera functionality. The secondary wireless device 130 may communicate wirelessly with the portable transaction device 102 using any type of wireless communications protocol. For example, the secondary wireless device 130 and the portable transaction device 102 may communicate using a Bluetooth type wireless link 132.

Where a one-time use transaction number is employed, the number may be generated by the card issuer or locally by the portable transaction device 102. Generation of the single-use number may be accomplished in one of several ways. For example, when an account is issued the card holder may get several pre-assigned surrogate numbers. The numbers will also have a pre-specified sequence. This sequence is known to the issuing bank and the user's portable transaction device 102. The issuing bank will authorize payments only based on the expected sequence of account numbers. If out-of-sequence account numbers are used, then the issuing bank will consider that transaction as a potential theft. The issuing bank can also use this feature to track the merchant involved in the potentially fraudulent transaction.

According to another example, a pre-assigned sequence can be reset to the original starting number on the list depending on user input or other triggers. In addition, the list of numbers can be downloaded via the mobile phone network on a regular basis. This can enhance security by minimizing the potential for repetitive number lists.

Regardless of the particular method, upon receipt of the surrogate card number, the merchant typically sends the surrogate card number to the card issuer for authorization/validation. Merchants do not need to install additional software to receive surrogate card numbers or to transmit them to card issuers. When the card issuer receives the account number, it is flagged as a single-use number and decoded to reveal the cardholder's standing account number. An authorization or denial is attached to the account number, which is recoded back to the temporary account number and sent to the merchant. Any attempt to reuse a surrogate card number outside the parameter results in denied authorization. In addition to or instead of these examples, other methods for generating one-time use numbers may be employed.

In conducting a transaction, the user, possessing both the secondary wireless device 130 and the portable transaction device 102, may press a control button 108 on the portable transaction device 102 requesting that the card 120 or electronic stripe 104 be readied with a new one-time use transaction number. The electronic stripe 104 may be selected by the user for use in swipe-type card readers, and the card 120 may be selected for either swipe-type card readers or insertion-type card readers, such as ATMs. It will be appreciated that the device 102 may be manufactured with only an electronic stripe, or only a card reader, rather than both. It will be further appreciated that the card 120 may include a reprogrammable magnetic stripe, a reprogrammable electronic stripe, or may be a so-called "smart" card with a reprogrammable internal memory, and the portable transaction device 102 may be configured to interface and reprogram one or more of these types of cards.

It should be appreciated that the portable transaction device 102 may be implemented in a variety of different configurations. For example, as described at length below and shown below in an alternate system depiction (Fig. 2), the

portable transaction device may be implemented as, or in connection with, a mobile telephone.

Fig. 2 shows a transaction system with multi-factor authentication. Transaction system 200 includes transaction processing server 150, point-of-sale (POS) transaction card reader 140, mobile telephone 202, removable and reprogrammable card 205, and secondary wireless device 130. Mobile telephone 202 is an example of a portable transaction device, and any reference made herein to a portable transaction device is meant to include mobile telephones as well as other portable transaction device embodiments.

The mobile telephone 202 may include a camera (video and picture) component 114, a biometric (e.g., fingerprint) scanner 112, a display 110, a voice (microphone and speaker) component 106, and controls 108. The mobile telephone 202 may also include voice-activation and camera functionality. The secondary wireless device 130 may communicate wirelessly with the mobile telephone 202 using any type of wireless communications protocol. For example, the secondary wireless device 130 and the mobile telephone 202 may communicate using a Bluetooth type wireless link 132. Further, the mobile telephone may communicate with a cell network, shown by signal 232.

Removable and reprogrammable card 205 may be utilized in many ways. For example, removable and reprogrammable card 205 may be left in the mobile telephone 202 for use in swipe-type card readers, or may be removed from mobile telephone 202 for use with insertion-type card readers. Examples of insertion-type card readers include automatic teller machines (ATMs).

In the example of Fig. 2, the mobile phone 202 provides all the functionality of the previously-described portable transaction device 102 (Fig. 1). In addition, the ability of the mobile phone 202 to access a communications network (e.g., the cell phone network) may be used to provide additional functionality. For example, if the cell phone is lost, a call can be placed through the network to disable all financial card functions. If the key fob is lost, a new key fob can be mailed to the user and the configuration information can be updated automatically by placing a call through the cell phone network.

Regardless of the particular configuration, the system may be configured to eliminate or reduce fraudulent transactions by performing multiple

authentications of each transaction, as follows. Possession of the portable transaction device provides a first factor of authentication. Second, the fingerprint of the user may be scanned and checked against a fingerprint stored in memory on the device. Third, at the time of the transaction, the wireless link to the secondary wireless device may be checked to verify that the secondary wireless device is communicating a proper device ID to the portable transaction device, thus indicating that the secondary wireless device is located within a predetermined distance of the portable transaction device. If these authentication steps are satisfied, the electronic stripe or card is reprogrammed with a one time use transaction number. In addition, the portable electronic device may store information pertaining to multiple different cards, and the user would be allowed to supply an input specifying which of the cards would be designated for use in the upcoming transaction.

Once the card is readied for use after authentication and any required user input, the user or a store clerk may swipe the electronic stripe through a swipe-type card reader, remove the card from the device and swipe it in a swipe-type card reader, or feed it into an insertion-type card reader, such as found on an ATM. As an additional authentication step, the one-time use transaction number may be checked by the transaction processing server for validity.

As described above, various embodiments of the present invention provide multi-factor authentication. For example, various embodiments of the invention may use two or three factor authentication for access control and information or identity theft prevention of financial card, bank check, electronic and computing devices. Two-factor authentication is defined as providing access based on validating whether the user has access to at least two verifiable pieces of information that are truthful and are available only to him/her. An example of two factor authentication is having access to a debit card and knowing the correct PIN number to complete a debit card transaction. Similarly, three-factor authentication is defined as providing access based on validating whether the user has access to at least three verifiable pieces of information that are truthful and are available only to him/her.

The following is an outline of various system elements that may be used in implemented various embodiments of the described systems and methods. It

will be appreciated that no single element is essential to every possible exemplary embodiment.

1. Portable transaction device (e.g., portable telephone)

A. Wireless interface configured to detect secondary wireless device when within predetermined distance (e.g. Bluetooth)

B. Fingerprint scanner

C. Memory storing fingerprint data of authorized user

D. Display (optional)

E. Controls for reprogramming card/stripe

F. Card insertion slot

G. Electronically reprogrammable stripe

H. Camera functionality: when the portable transaction device is activated, a photograph of the user may be taken. The photograph may be send to the card issuer and/or displayed on the portable transaction device during use to provide additional security (e.g., a fourth authentication factor)

I. Voice-activation functionality

2. Wireless secondary device (e.g. key fob)

A. Wireless link to portable transaction device

3. Card

A. Magnetically programmable stripe OR electronically programmable stripe, OR electronically programmable internal memory (so called smart card)

B. Configured to be inserted into portable transaction device and programmed with a one-time use card number on a per-transaction basis

4. Point of Transaction Card Reader

5. Transaction Processing Server

6. Authentication factors (may be implemented in varying combinations) to determine if a pending transaction is fraudulent

A. Wireless secondary device within predetermined range of portable transaction device

B. Scanned fingerprint matches stored fingerprint

C. Single-use transaction number written to card is valid

Figure 3 shows a block diagram of a programmable card. Programmable card 300 may be utilized as removable and reprogrammable card 205 (Figure 2). Programmable card 300 includes thin profile battery 302, power management circuitry 304, microcontroller with flash 306, Bluetooth front end 310, Bluetooth antenna 312, universal serial bus (USB) and power supply connector 322, and display driver 320.

Figure 4 shows a block diagram of a secondary wireless device. Secondary wireless device 400 may be utilized as secondary wireless device 130 (Figures 1, 2). Secondary wireless device 400 includes thin profile batttery 402, power management circuitry 404, microcontroller 406, read only memory (ROM) 420, FLASH memory 408, Bluetooth front end 410, Bluetooth antenna 412, and USB and power supply connector 422.

Figure 5 shows a computer and base station. Computer 510 may be any type of computer or computing device capable of being operated by a user and being coupled to base station 520. For example, computer 510 may be a personal computer, a handheld computer, or the like. Computer 510 may include software to drive the base station and its components, and may also include graphical user interface (GUI) front end software for step-by-step user instructions for programming a reprogrammable card. As described above, programming a reprogrammable card may include selection of rolling numbers and associated maximum transaction amounts.

As shown in Figure 5, base station 520 includes universal serial bus (USB) interface 528, card reader 522, secondary wireless device slot 526, and a reprogrammable card slot 524. Base station 520 may communicate with computer 510 over a cable coupled to USB interface 528. Although interface 528 is shown as a USB interface, this is not a limitation of the present invention. Any suitable interface may be used without departing from the scope of the present invention.

Base station 520 provides an interface between computer 510 and one or more other items. For example, in some embodiments, a reprogrammable card may be placed in slot 524 for communications with computer 510, or for programming by computer 510. Further, in some embodiments, a secondary wireless device may be placed in slot 536 for communications with computer

510, or for programming by computer 510. Also in some embodiments, base station 520 may be used for charging a reprogrammable card and secondary wireless device.

Base station 520 may also be used for reading standard magnetic cards to store information into a reprogrammable card. For example, a reprogrammable card may be placed in slot 524, and one or more standard magnetic cards may be swiped through card reader 522. Base station 520 may include circuitry to program a reprogrammable card directly from swiped magnetic cards, or may program a reprogrammable card under the control of computer 510.

Figure 6 shows usage models for various embodiments of the present invention. Figure 6 shows user icons to represent users in various stages of use, and arrows to indicate actions. The various usage models are now described. At 602, an un-programmed reprogrammable card, a secondary wireless device, and a base station are shipped to a user. Software on CD-ROM and an optional travel kit may also be shipped to the user. At 604, the user 612 installs the software and connects the base station to a home personal computer (PC). The software is run to initiate programming, and the user scans a fingerprint into the reprogrammable card. The user plugs the reprogrammable card and the secondary wireless device into the base station.

At 614, the software communicates with a server 622 to activate the reprogrammable card and secondary wireless device. Server 622 may be held at a secure location separate from the user and from a card issuing bank 660. For example, server 622 may be held by a company that provides reprogrammable cards and secondary wireless devices. Further, information may be stored on the server 622 for retrieval in case of loss of the reprogrammable card or secondary wireless device. The user 612 may then scan one credit card at a time into the base station. This may be repeated any number of times. The user 612 is shown at a PC performing the actions just described.

At 618, the user 642 has completed the setup, and has a reprogrammable card available for use. The user 642 carries both the reprogrammable card and the secondary wireless device. It is best to keep the secondary wireless card separate from the reprogrammable card. The secondary wireless device never has to be accessed by user 642 to initiate a transaction. At the end of the day, the

user 642 plugs the reprogrammable card and the secondary wireless device into the base station for charging and account summary.

At 644, user 670 initiates a transaction with merchant 672. To initiate the transaction, user 670 activates the reprogrammable card using a fingerprint scan and selects the credit card to use. The reprogrammable card authenticates only in the presence of the appropriate secondary wireless device. Information programmed on the reprogrammable card's electronic stripe will get erased automatically after a predetermined timeout. For example, the information may get erased after five minutes. To prevent multiple swipes, the information in the reprogrammable card may be erased after one swipe. An alternative is to provide a rolling account number that the credit card company can map to the actual account number. The account number may then roll to a new number for each fingerprint scan.

If a user 652 loses one of the reprogrammable card or secondary wireless device, shown by 654, the company will mail a preprogrammed reprogrammable card or secondary wireless device to the user 652 at 624. If a user 632 loses both the reprogrammable card and secondary wireless device, shown by 616, the company will help deactivate all user credit card accounts and start the process again at 634.

As described above, reprogrammable cards may take any suitable form. For example, reprogrammable cards may be magnetic stripe cards, electronically programmable cards, smart cards, or any combination. Various embodiments are now described under headings relating to magnetic cards, electrically programmable cards, and smart cards. It should be noted that nothing in these embodiments should be considered essential.

Magnetic stripe cards

Embodiments that include magnetic stripe cards are now described with reference to Figures 1-6. Various embodiments of the present invention include: (i) an intelligent (memory, computational power) electronic device that has magnetic stripe reading / writing capability, and a wireless link such as Bluetooth; (ii) a fingerprint scanner on the intelligent electronic device; (iii) electronic device such as a key that has memory and wireless connection such as

Bluetooth; and (iii) an empty generic three track magnetic stripe card that can be programmed by the intelligent electronic device on a per transaction basis. For example, Figures 1 and 2 show portable transaction devices 102 and 202 that may be used as intelligent electronic devices. Further, portable transaction devices 102 and 202 are shown having wireless links and fingerprint scanners. Portable transaction device 202 is shown having a magnetic stripe reader/writer to program reprogrammable card 205.

The use of an intelligent electronic device with a fingerprint scanner or the use of an intelligent electronic device and the key (secondary wireless device) constitutes a two-factor authentication solution while the use of all three (intelligent electronic device with the fingerprint scanner and the key) constitutes a three-factor authentication solution.

The user first installs interface software in the intelligent electronic device. Using the installed software the user scans his/her portfolio of standard financial cards using the integrated magnetic stripe card reader. The user may also enter information necessary for financial card transactions that may not be present in the magnetic stripe such as a security code. The user also scans a fingerprint to associate the cards with the user. The financial card information is stored in the intelligent electronic device in encrypted form. The decryption code for the information stored in the intelligent electronic device may be stored in the key. Each intelligent electronic device may have an associated key that is unique. Once all the relevant information is stored in the intelligent electronic device, the user may slide the generic card into the integrated magnetic stripe reader/writer.

When the user is ready to use a financial card for a transaction s/he logs into the intelligent electronic device using the fingerprint scanning device or by entering a password. In the two-factor solution, the card user can proceed with initiating the transaction. In the case where the user opts for a three-factor solution, the intelligent electronic device will let the login occur only if it is able to establish a wireless link with its associated key. The user then selects the type of card to use. After log in using either approach, the intelligent electronic device receives the decryption code from the key to access the information about the selected card, if key based authentication is used. If fingerprint scan based

authentication is used for two-factor then the decryption code is stored in the intelligent electronic device itself, which will be provided after the authentication. The user then pulls out the generic card, during which the card is programmed by the magnetic writer. At this point the intelligent electronic device deletes the decryption key information that it received from the key. Once programmed, the generic card can be used like any other magnetic stripe financial card. Once the transaction is completed the user inserts the card back into the intelligent electronic device during which the information stored in the magnetic stripe is erased.

Further embodiments may be generated by combining various feature of magnetic card embodiments with electronically programmable embodiments and smart card embodiments, described below. The use of magnetic cards as reprogrammable cards may obviate the need for a power supply in the card, and provides a mechanism to use traditional three track magnetic stripe cards and hence does not require development of a card that has an alternate programming medium.

Note that the need for having access to the intelligent electronic device along with fingerprint scanning and the presence of a key provides a three-factor authentication. The same can be implemented without the key in which case the security of the information stored in the intelligent electronic device may be achieved with two-factor authentication through fingerprint scanning. The key can also be replaced with a PIN input + fingerprint scanning; however, without the key the decryption code is physically stored in the same device as that of the information. A key along with the intelligent electronic device can be used as two-factor authentication.

Electronically programmed cards

Embodiments that include electronically programmable cards are now described with reference to Figures 1-6. Various embodiments of the present invention include: (i) a base station having the ability to scan a user's card information; (ii) an electronic card that has an electronically programmable region that has identical dimensions as that of a magnetic stripe (henceforth referred to as the electronic stripe), a wireless link such as Bluetooth and a

fingerprint scanner; (iii) an electronic device such as a key that has memory and a wireless link such as Bluetooth. For example, Figures 1 and 2 show portable transaction devices 102 and 202 that may be used as intelligent electronic devices. Further, stripe 104 (Figure 1) may be a reprogrammable electronic stripe, and stripe 204 (Figure 2) may be a reprogrammable electronic stripe. Note that the electronic programming may be done using electric currents. The direction of current travel will change the magnetic field and hence can be used to code for a digital "1" or a digital "0". This information can then be read by a traditional magnetic stripe reader present in point-of-sale.

The electronic card may come preprogrammed with software that will allow users to input card information or the users may first install interface software in the intelligent electronic device or in the base station. Using the installed software the user will then enter standard financial card information. An optional card reader can be used to read most of the information present in a financial card. The financial card information will be stored in the intelligent electronic device in encrypted form. The decryption code for the information stored in the intelligent electronic device will be stored in the key. Each intelligent electronic device will have an associated key that is unique.

When the user is ready to use a financial card for a transaction s/he logs into the intelligent electronic device using a fingerprint scanning device or by entering a password. In the two-factor solution, the card user can proceed with initiating the transaction. In the case where the user opts for a three-factor solution, the intelligent electronic device will let the login occur only if it is able to establish a wireless link with its associated key. The user then selects the card to use through a card selection button on the face of the intelligent electronic device. The intelligent electronic device receives the decryption code from the key to access the information about the selected card. The intelligent electronic device programs the electronic stripe. At this point the intelligent electronic device deletes the decryption key information that it received from the key. Once programmed the intelligent electronic device can be used like any other magnetic stripe financial card. Once the transaction is completed, the intelligent electronic device erases the information stored in the electronic stripe. The

electronic stripe can be programmed to time out after a certain length of time or after a specified number of swipes.

In some embodiments, the key may store all critical information from the intelligent electronic device as backup in encrypted format. The decryption code for information stored in the key may be present in its associated intelligent electronic device. Also in some embodiments, an intelligent electronic device may include software having the ability for the intelligent electronic device to either limit to one swipe after programming or record how many times a card was swiped between magnetic stripe programming and erasing. In further embodiments, the intelligent electronic device may include software and/or voice recognition that tracks the expenses based on user input every time the card is used or when the user makes any expense transaction to provide categorized expense summary. In further embodiments, the intelligent electronic device may include the ability to communicate to the point-of-sale the amount entered by the user for transaction – this however will require change to the point-of-sale. In still further embodiments, the intelligent electronic device may include the ability to generate one account number from a set of account numbers. These numbers will be generated in a predetermined sequence (or one time use numbers) that will expire at the end of every transaction to eliminate card cloning and counterfeiting operations. In some embodiments, this may be achieved by either using the 19 digit PAN Field and/or Discretionary Data character fields allocated in the magnetic stripe standards. For example, the way the variable number (required for off-line transactions) would work is that a card holder may be assigned let us say 100 account numbers. The account numbers will revolve in a pre-determined order. The issuing bank will know what order will be used and so will the intelligent electronic device. For each authentication the intelligent electronic device will activate one number in the pre-determined order. The variable number also applies for on-line transactions and can either replace or work with the one time use numbers.

In some embodiments, the programmed magnetic stripe may be detached from the main unit for use in transactions where the card is swallowed in whole to complete the transaction (such as in an ATM machine or at a gasoline pump). Also in some embodiments, a fixed base station may be connected to a desktop

PC or a standalone base station and can be used for charging the intelligent electronic device and key. The base station may also be used to retrieve financial card information for the desktop PC from the intelligent electronic device for electronic transactions. The transaction will occur only if both the intelligent electronic device and key are present. The fixed base station may also be used to include the optional magnetic card reader to initially download the information into the intelligent electronic device. In some embodiments, an organic light emitting diode (LED) display and flexible printed circuit board (PCB) may be used to design an intelligent electronic device that has the form factor and mechanical flexibility of a plastic card so that it can be carried inside a wallet. The intelligent electronic device may also act as an agent that holds other secure information such as user ID and password for access by the user after two or three factor authentications. Further, an intelligent electronic device that is enabled with wireless may be used to show on-demand advertisement and coupons on its display. The information displayed can depend on the card holder's usage pattern, if available.

For card-not-present on-line transactions, the mode of operation may be one of the following: (a) base station will verify the presence of the intelligent electronic device along with two or three factor authentication, explained above, or (b) if random or one-time use numbers are used, then with two or three factor authentication the intelligent electronic device will provide the correct number to use for card-not-present transactions similar to card present transactions.

In electronically programmable embodiments, the user does not have to deal with a third component, the generic card, unlike the magnetic card options described above. Further, the erasing of the information stored in the electronic stripe may be automatic, whereas in the magnetic card embodiments, erasing may depend on the user sliding the generic card back into the intelligent electronic device.

Note that the need for having access to the intelligent electronic device along with fingerprint scanning and the presence of the key provides a three-factor authentication. The same can be implemented without the key in which case the security of the information stored in the intelligent electronic device is achieved with two-factor authentication through fingerprint scanning. The key

can also be replaced with a PIN input + fingerprint scanning to result in three-factor authentication. However, without the key the decryption code is physically stored in the same device as that of the information and therefore susceptible to theft by hacking. The key along with the intelligent electronic device may be used as two-factor authentication.

Although the various embodiments of the present invention are described above using an intelligent electronic device and key, other devices may be utilized. For example, an intelligent electronic device may be a self powered smart card device that includes a display, fingerprint reader, and Bluetooth. Further, PIN entry or other biometric authentication can be used instead of fingerprint authentication.

Smart cards

Embodiments that include smart cards are now described with reference to Figures 1-6. Various embodiments of the present invention include: (i) an electronic device such as a personal digital assistant or an intelligent electronic device with smart card interface and wireless link such as Bluetooth; (ii) an electronic device such as a key that has memory and wireless link such as Bluetooth; (iii) the ability to generate predefined card numbers at random that will expire at the end of every transaction to eliminate card cloning and counterfeiting operations; and (iv) an empty generic smart card that can be programmed by the intelligent electronic device. The assumption here is that the point-of-sale uses smart cards.

The usage model is similar to that described above with reference to magnetic stripe cards, except the Intelligent Electronic Device programs the smart card instead of the magnetic stripe card.

In some embodiments, the intelligent electronic device and the smart card may be integrated into one device. This will result in a device similar to devices described above with reference to electronically programmed cards, except it is to be used for smart card point-of-sale.

Further, in some embodiments, a standalone smart card may be utilized without the intelligent electronic device. Each smart card will have an associated key. The smart card point-of-sale will verify if the associated key is

present before approving the transaction. One feature of these embodiments is that the smart card is not programmable to act as one of several cards and will require change in the point-of-sale.

Although the various embodiments of the present invention are described above using an intelligent electronic device and key, other devices may be utilized. Further, PIN entry or other biometric authentication can be used instead of fingerprint authentication.

Various embodiments described thus far include "programmable" financial cards, where "programmable" refers to the fact that the information for the card's stripe is programmable to represent one of several cards held by the card holder. Embodiments are now described that are applicable to authentication for bank checks.

Authentication for bank checks

Figure 7 shows an intelligent electronic device capable of printing checks. Intelligent electronic device 700 includes storage 744 for "blank" paper checks without account information, a wireless interface to support a wireless link 732 such as Bluetooth, a fingerprint scanner 712, a display screen 710, account selection and function buttons 708, and a miniature printer 742 to print checks. Also shown in Figure 7 is a key 730 that has memory and a wireless link such as Bluetooth.

The intelligent electronic device 700 will be preprogrammed with relevant account (or accounts) information including account holder name, mailing address, account number, and bank routing number. When the user is ready to use the check book s/he will power up the intelligent electronic device. The device will authenticate the user by verifying the presence of the key and/or fingerprint ID. Once authenticated, the user will pick the account of choice and optionally enter memo along with the transaction amount information. The printer then will print the account and transaction information on the blank paper check to produce a printed check 740. Any features discussed above with reference to programmable card embodiments may utilized with intelligent electronic device 700 without departing from the scope of the present invention.

Further, PIN entry or other biometric authentication can be used instead of fingerprint authentication.

Financial Card Transaction Verification

Figures 8-10 show various methods for financial card transaction verification in accordance with various embodiments of the present invention. Figure 8 shows an example of "real time push verification," Figure 9 shows an example of "offline push verification," and Figure 10 shows an example of "offline pull verification." The embodiments represented by Figures 8-10 are applicable for all programmable financial card embodiments described herein and for all other standard cards.

When a transaction is initiated from the point-of-sale, credit card and transaction information is transferred to an acquirer 802 and a card issuing bank 804. These transfers are shown at 812 and 822 in Figures 8-10. The card issuing bank 804 transfers an approval or denial of the transaction to the acquirer 802 and ultimately to the point-of-sale. The transfers are shown at 824 and 814 in Figures 8-10. The acquirer 802 typically pays the merchant after verification. The card issuing bank 804 then pays the acquirer 802.

In various embodiments of the invention, an additional step is added either during information processing at the acquirer or at the card issuing bank. This additional step involves instant messaging to the card holder's phone/email with the necessary transaction details, which then when approved by the card holder is recorded to be a legitimate transaction. The phone 806 can be a mobile phone running special software that indicates to the user that a new transaction has arrived for approval. If the approval is not completed within a prescribed time the transaction is marked as a possible suspect and further defensive actions can be taken. The transaction records on the mobile device 806 can be downloaded onto PC financial software for record keeping. This transfer is shown at 840. Access to mobile device instant messaging can be restricted via PIN entry, voice recognition, or other biometric authentication such as fingerprint.

Figure 8 shows a real time push verification where the issuing bank 804 sends a real time message 832 to the mobile device 806 and waits for approval or

denial at 834 before approving the transaction at 824. Figure 9 shows an offline push verification where the issuing bank 804 sends a message 832, but does not wait for real time approval. Instead, a user may provide later notification of approval or denial at 934, and if necessary, the issuing bank 804 may take defensive action.

In other embodiments, instead of the information being pushed via automated mobile phone instant message, it can be an information pull based implementation, such as that shown in Figure 10. In information pull implementations, the transaction details are logged on a secure web site 1008 where the user visits periodically to approve the transactions at 1034.

Figure 11 show a flexible form factor for a programmable financial card. Programmable financial card 1100 has a flexible printed circuit board (PCB) that may include embedded integrated circuit components such as memory, processing, display driver, and wireless front end. In addition, programmable financial card 1100 may include a fingerprint reader, input buttons, organic LED display, and flexible battery power.

Figure 12 shows a perspective exploded view of the programmable financial card of Figure 11. Programmable financial card 1100 includes flexible PCB 1202, programmable stripe 1204, organic LED display 1216, and fingerprint input device 1214. Flexible PCB 1202 includes flexible battery 1208, battery charging by contactless coupling 1206, memory, processing, and display driver integrated circuits 1210, and wireless front end integrated circuit and antenna 1212.

Figure 13 shows usage models for a secondary wireless device in card-present transactions and card-not-present transactions. Usage models for card-not-present transactions are show in the top portion of Figure 13, shown generally at 1302. In these embodiments, secondary wireless device 1310 communicates with various types of electronic devices that in turn communicate with point-of-sale terminals or merchants without a reprogrammable card present. For example, secondary wireless device 1310 may provide user transparent automated authentication with a home computer and base station 1320, laptop computer 1330, personal digital assistant (PDA) 1340, or cellular

telephone 1350. These devices may then in turn communicate with merchants using one or more secure protocols such as: Secure Electronic Transaction (SET), Mobile electronic Transaction (MeT); M-payments; or other emerging standards.

Usage models for card-present transactions are show in the bottom portion of Figure 13, shown generally at 1304. In these embodiments, secondary wireless device 1310 provides user transparent automated authentication with one or more of a reprogrammable card 1360 and portable transaction device 1370. Reprogrammable card 1360 may then communicate with point-of-sale terminals or merchants.

Multi-factor authentication may be utilized in both card-present and card-not-present transactions. For example, two factor or three factor authentication may be provided as described above with reference to Figures 1-6.

The following numbered paragraphs provide further disclosure of the systems and methods of the present description:

1. A financial transaction authentication system, including a mobile telephone (or handheld computer or other portable electronic device) having a biometric scanner and a transaction stripe that may be operatively engaged with a point-of-sale stripe reader, where the financial transaction authentication system is configured to combine biometric information with one or more additional authentication factors to secure financial transactions.

2. The system of paragraph 1, where the stripe is attached to the mobile telephone.

3. The system of paragraph 1, where the stripe is provided on a separate structure (e.g., a structure shaped and sized like a traditional financial card) that may be selectively inserted into and removed from the mobile telephone.

4. The system of paragraph 1, further comprising software configured to control financial transaction communication between the mobile telephone and various external systems involved in financial transaction, and configured to control communications between the mobile telephone and access controls implemented in buildings, cars etc.

5. The system of paragraph 1, further comprising software configured to implement and apply one-time use numbers on to the transaction stripe, wherein this may include local generation of the one-time use numbers or download of one-time use numbers via a mobile telephone network.

6. The system of paragraph 1, where the information is encoded onto the transaction stripe via electrical voltage pulses that generate magnetic fields to mimic magnetic stripe tracks in standard financial transaction cards. The sequence of pulses of time duration T and 2T may be used to code for 1 and 0. Since the pulse train is not stored magnetically the stripe length can be much smaller than that of a standard card. The card substrate can thus be much smaller than a traditional financial card. The card may include the transaction stripe, optional memory and optional energy storage to support complete detaching from the mobile telephone. The detachable card may also include wireless capability to communicate to the mobile telephone.

7. The system of paragraph 1, where in multi-factor authentication, biometric data (e.g., fingerprint) is used to access the mobile phone device and PIN entry is required to access account information.

8. The system of paragraph 1, further comprising a secondary wireless device, such as a key fob, that is used to provide an additional authentication factor, namely that the mobile telephone will not allow access to the financial card account information unless the secondary wireless device is in the vicinity. Wireless key can be implemented via bluetooth protocol as an example.

9. The system of paragraph 1, where the mobile telephone is employed as a wireless authentication key for two factor authentication in accessing other electronic systems such as laptops, PCs, cars etc.

10. The system of paragraph 1, where the mobile telephone is used for card consolidation, in that information for multiple accounts is stored within a memory in the mobile telephone, and where the user may select a particular account and after proper authentication, the account information for the selected account is applied to the transaction stripe.

11. The system of paragraph 1, where since the system may be configured to require two or more factor authentication for gaining access to

account information, the system may be employed for secure card present and card not present transactions. Also, since the one-time use number generation is integrated into the mobile telephone, card present or card not present solutions can take advantage of this security feature.

12. The system of paragraph 1, where since the information on the electronic stripe is not coded in physical locations on the magnetic stripe more bits can be conveyed to the POS between the start and the stop sentinels. These additional bits can be used to have unique ID independent of any account information. This will ensure that even if account information is stolen without this unique ID in the stripe the transaction will not be valid. So a cloned card based on known account information will not make the transaction valid without this unique ID.

13. The system of paragraph 1, where since the mobile telephone device is connected to a mobile phone network, the account holder can set a per-transaction amount limit and if a transaction exceeds that limit the user will receive a secure SMS message (or a message via any other mobile network-based messaging service) requesting validation of the transaction; the transaction will be authenticated only after the user replies the SMS with an 'overlimit' password; the password will be independent of other passwords. Note that the per-transaction limit could be zero, which will require secure SMS authentication every transaction; also, if the mobile phone is not in a cell then the financial card issuing bank will note it as a 'risky' transaction and take appropriate action, such as invalidate the account for future transaction.

14. The system of paragraph 1, where since the mobile telephone device is connected to the mobile phone network, the account activation may happen via the mobile network after 2- or 3-factor authentication. Authentication may also happen via the mobile phone network; for example, a user will have to make a phone call and the system will verify the user's voice; once the voiceprint is verified, the mobile network will be used to download the financial card information onto the mobile telephone device.

15. The system of paragraph 1, where the mobile telephone device will also use the voice recording component in the mobile phones to record user voice keywords. The keywords will include the type of transaction and the

amount of transaction. The keywords can then be downloaded into a PC with voice recognition for automated data entry into software such as Microsoft Money or Quicken. The mobile telephone device can have two directional microphones, one for recording background noise and one for recording voice and background noise. This will improve voice recognition by canceling out background noise.

16. The system of paragraph 1, where the mobile phone network can also be used to upload account summary automatically from the card issuing bank. This can then be downloaded into a PC. All connections to the PC will be via an optional base station. The base station will also be used to charge the phone.

17. The system of paragraph 1, where the mobile phone network can also be used to update the cell phone service provider of the financial transaction details. This can be used to consolidate the mobile phone bill with the credit card transaction bill.

18. The system of paragraph 1, where since the mobile telephone device is connected to the mobile phone network, if the device is stolen the mobile phone network can be used to call the phone to delete all account information. Also, the network can be used to track a delinquent account holder.

19. The system of paragraph 1, where since the mobile telephone device is connected to the mobile phone network, gift cards and other stored value cards can be directly transmitted to a recipient if his/her telephone number is known.

20. The system of paragraph 1, where the mobile phone network can be used to upload user-specific ads/coupons into the mobile telephone device. This can also involve using Bluetooth or Infrared network to upload user specific ads/coupons.

21. The system of paragraph 1, where messages sent via the mobile phone network to and from the mobile telephone will be encrypted. Each mobile telephone device will have a unique private and public key which will be used for sending secure information.

22. The system of paragraph 1, where since the mobile telephone device provides secure storage of information, it can be extended to store not

such financial data but also other user information such as login IDs and passwords, account numbers for building access, user ID for access to cars, etc.

23. The system of paragraph 1, where the portable electronic device is configured to take photographs, and where a photograph of a user is taken during initial activation, and where such photograph is later employed to increase the security of a financial transaction (e.g., by providing an additional authentication factor).

24. The system of paragraph 1, where the portable electronic device is voice-activated.

25. The system of paragraph 1, where the transaction stripe is magnetically encoded via a magnetic head of the portable electronic device.

26. The system of paragraph 1, where the system is implemented using open technologies and specifications, such as ECML (electronic commerce modeling language).

27. The system of paragraph 1, where communications are secured via secure protocols such as TLS and SSL.

Although the present invention has been described in conjunction with certain embodiments, it is to be understood that modifications and variations may be resorted to without departing from the spirit and scope of the invention as those skilled in the art readily understand. Such modifications and variations are considered to be within the scope of the invention and the appended claims.

IPR2025-00644 Page 01162

What is claimed is:

1. A portable transaction device having a biometric scanner and a transaction stripe that may be operatively engaged with a point-of-sale stripe reader, where the portable transaction device is configured to combine biometric information with one or more additional authentication factors to secure financial transactions.

2. The portable transaction device of claim 1 wherein the transaction stripe may be selectively inserted into and removed from the portable transaction device.

3. The portable transaction device of claim 1 further comprising a wireless interface to communicate with a secondary wireless device for an additional authentication factor.

4. The portable transaction device of claim 1 further comprising controls to allow a user to select one of a plurality of financial cards with which to program the transaction stripe.

5. The portable transaction device of claim 1 further comprising software configured to apply one-time use numbers on to the transaction stripe.

6. The portable transaction device of claim 5 further comprising software for local generation of the one-time use numbers.

7. The portable transaction device of claim 5 further comprising software to download the one-time use numbers via a mobile telephone network.

8. A financial transaction apparatus comprising:
means for interacting with a user to provide a first authentication factor;
means for interacting with a secondary wireless device to provide a second authentication factor; and

means for communicating financial transaction information to a point-of-sale.

9. The financial transaction apparatus of claim 8 wherein the means for interacting with a user comprises a biometric input device.

10. The financial transaction apparatus of claim 9 wherein the biometric input device comprises a fingerprint scanner.

11. The financial transaction apparatus of claim 8 wherein the means for communicating financial transaction information comprises a reprogrammable stripe.

12. The financial transaction apparatus of claim 11 wherein the reprogrammable stripe comprises a programmable magnetic stripe.

13. The financial transaction apparatus of claim 11 wherein the reprogrammable stripe comprises an electronically programmable stripe.

14. The financial transaction apparatus of claim 11 wherein the reprogrammable stripe comprises a smartcard interface.

15. A financial transaction authentication system comprising:

a reprogrammable card having a programmable transaction stripe that may be operatively engaged with a point-of-sale stripe reader; and

a secondary wireless device to provide user authentication, wherein both the reprogrammable card and secondary wireless device are configured to communicate with a portable transaction device.

16. The financial transaction authentication system of claim 15 further comprising the portable transaction device.

17. The financial transaction authentication system of claim 15 wherein the programmable transaction stripe comprises a programmable magnetic stripe.

18. The financial transaction authentication system of claim 15 wherein the programmable transaction stripe comprises an electronically programmable stripe.

19. The financial transaction authentication system of claim 15 wherein the programmable transaction stripe comprises a smartcard interface.

20. The financial transaction authentication system of claim 15 wherein the secondary wireless device comprises a key fob.

IPR2025-00644 Page 01165

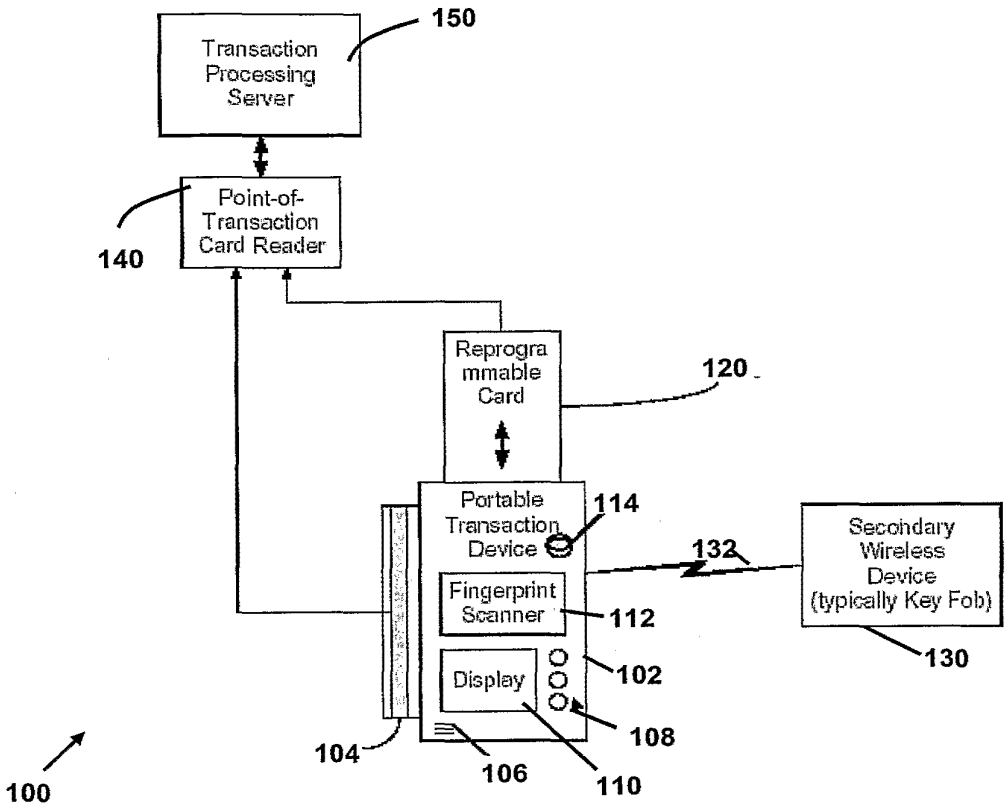

Transaction Processing Server
150
Point-of-Transaction Card Reader
140
Reprogra mmable Card
120
Portable Transaction Device
114
Fingerprint Scanner
112
Display
102
108
110
106
104
100
132
Secondary Wireless Device (typically Key Fob)
130

Fig. 1

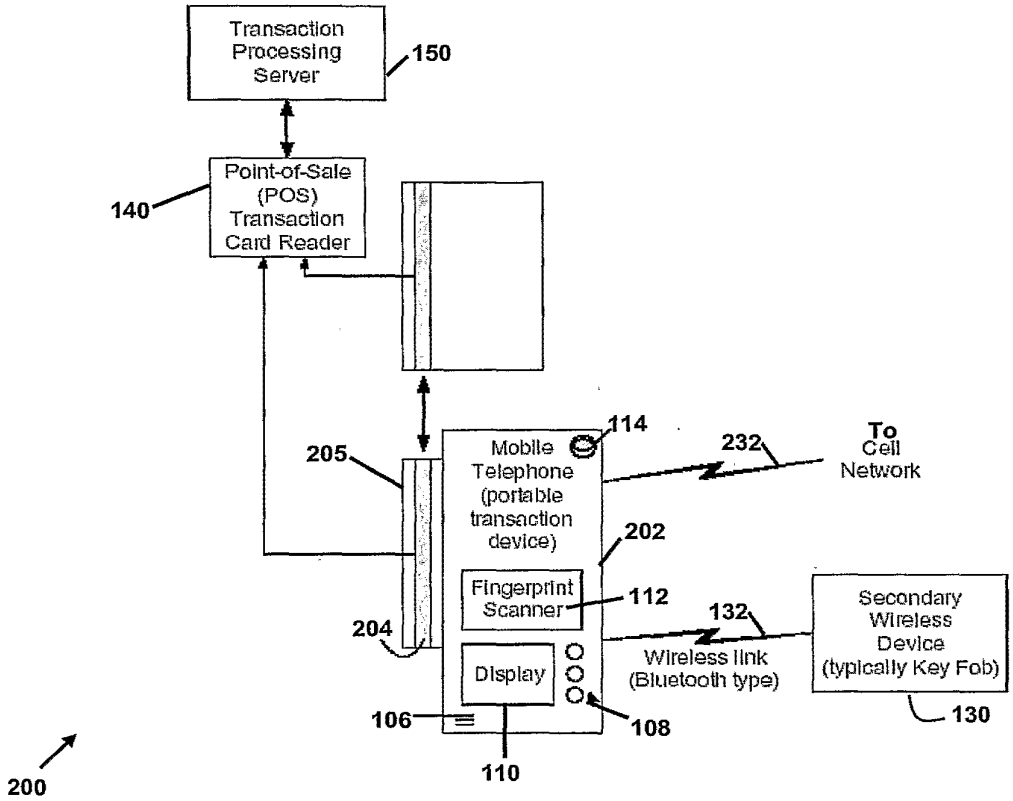

Transaction Processing Server
150
Point-of-Sale (POS) Transaction Card Reader
140
205
Mobile Telephone (portable transaction device)
114
232
To Cell Network
202
Fingerprint Scanner
112
204
132
Secondary Wireless Device (typically Key Fob)
Wireless link (Bluetooth type)
Display
106
108
130
110
200

Fig. 2

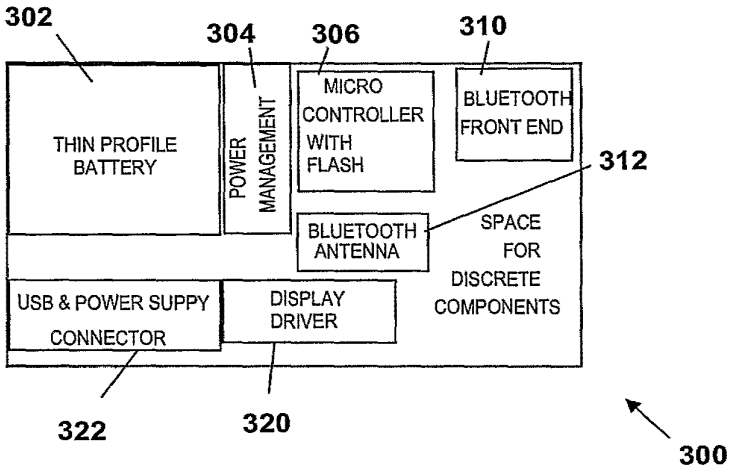

302
304
306
310
THIN PROFILE BATTERY
POWER MANAGEMENT
MICRO CONTROLLER WITH FLASH
BLUETOOTH FRONT END
312
BLUETOOTH ANTENNA
SPACE FOR DISCRETE COMPONENTS
USB & POWER SUPPY CONNECTOR
DISPLAY DRIVER
322
320
300

Fig. 3

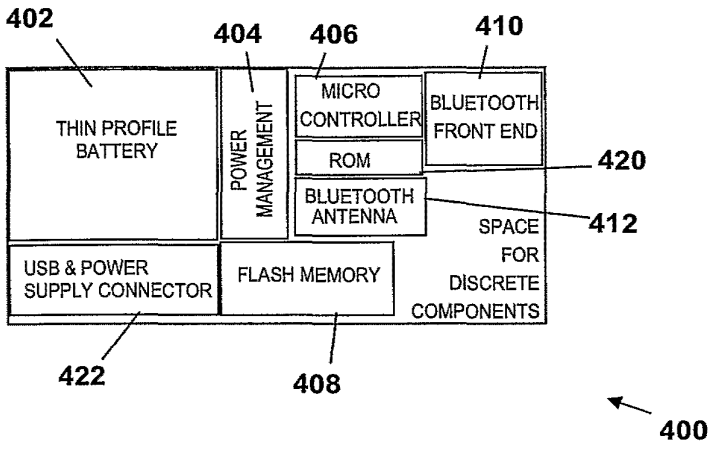

402
404
406
410
THIN PROFILE BATTERY
POWER MANAGEMENT
MICRO CONTROLLER
BLUETOOTH FRONT END
ROM
420
BLUETOOTH ANTENNA
412
SPACE FOR DISCRETE COMPONENTS
USB & POWER SUPPLY CONNECTOR
FLASH MEMORY
422
408
400

Fig. 4

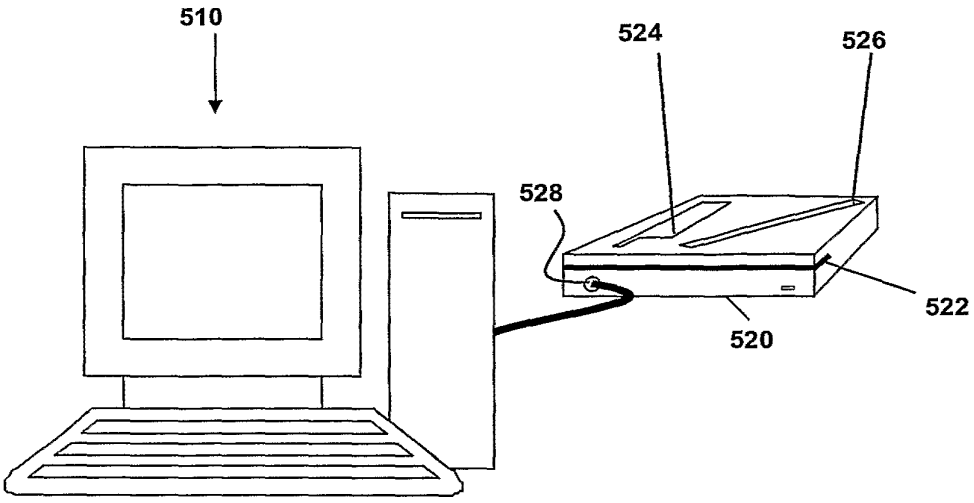


Fig. 5

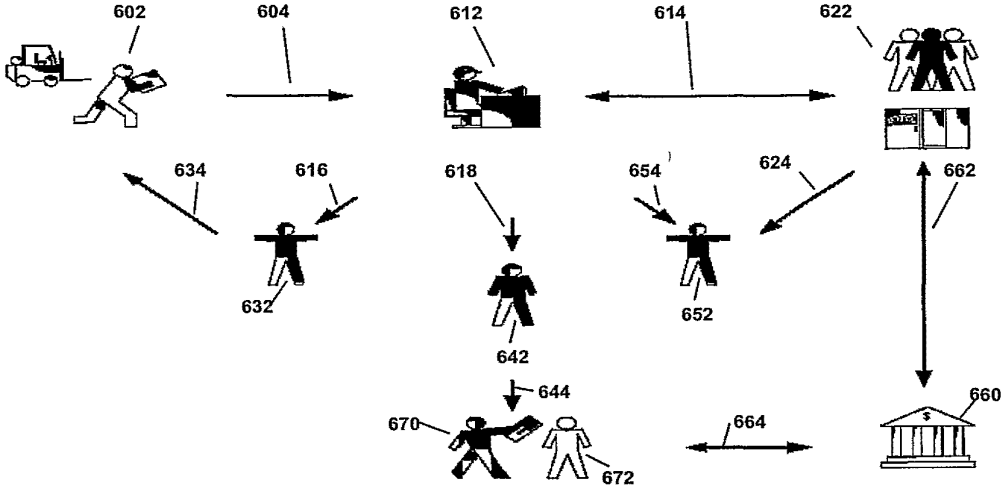

602
604
612
614
622
634
616
618
654
624
662
632
642
652
644
660
670
664
672

Fig. 6

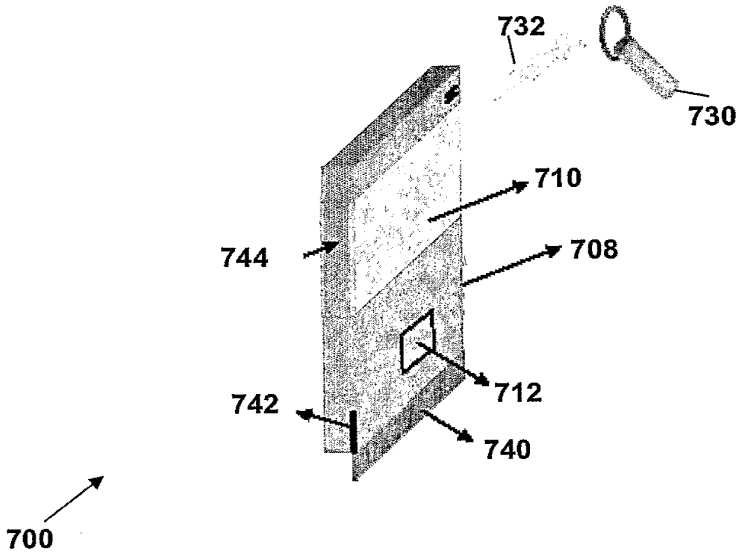


Fig. 7

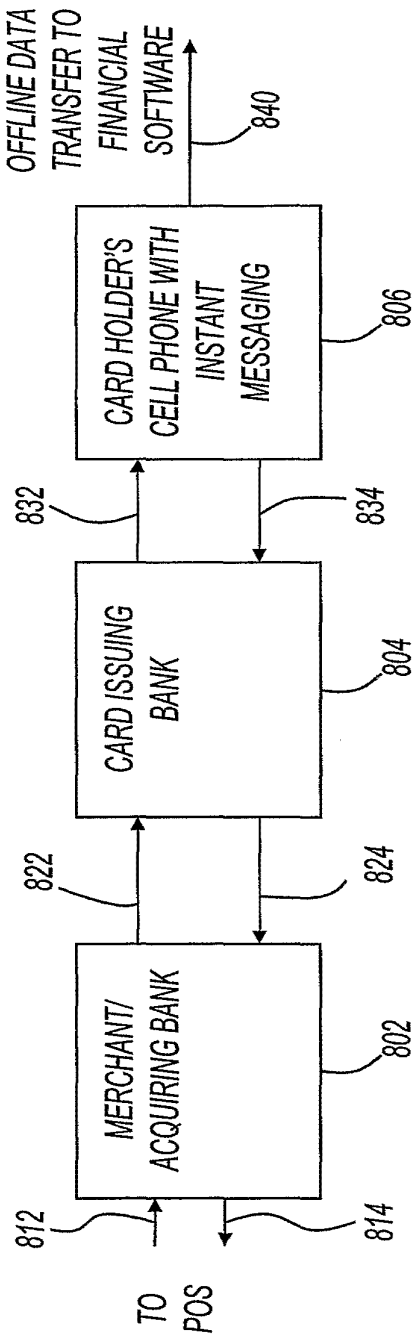

OFFLINE DATA TRANSFER TO FINANCIAL SOFTWARE
840
CARD HOLDER'S CELL PHONE WITH INSTANT MESSAGING
806
832
834
CARD ISSUING BANK
804
822
824
MERCHANT/ ACQUIRING BANK
802
812
814
TO POS

FIG. 8

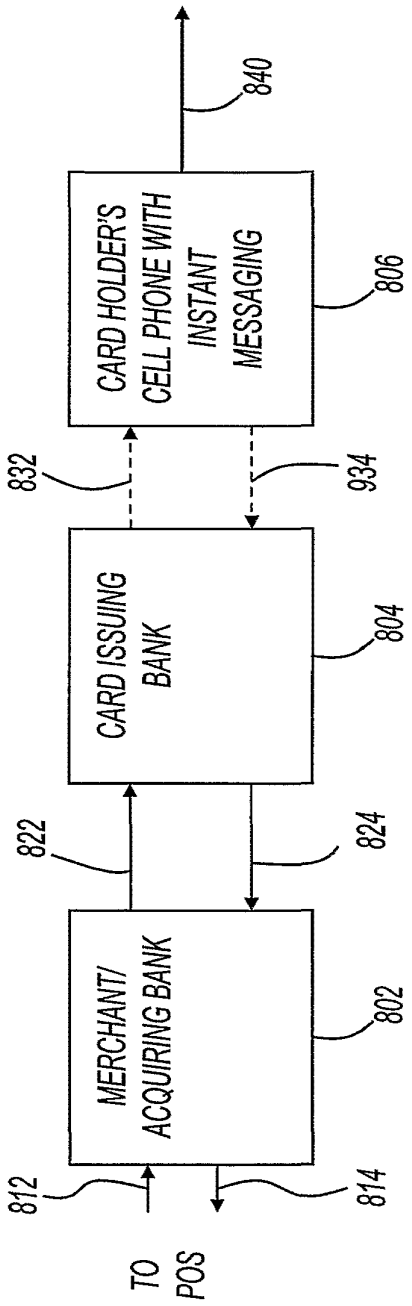

840
CARD HOLDER'S CELL PHONE WITH INSTANT MESSAGING
806
832
934
CARD ISSUING BANK
804
822
824
MERCHANT/ ACQUIRING BANK
802
812
814
TO POS

FIG. 9

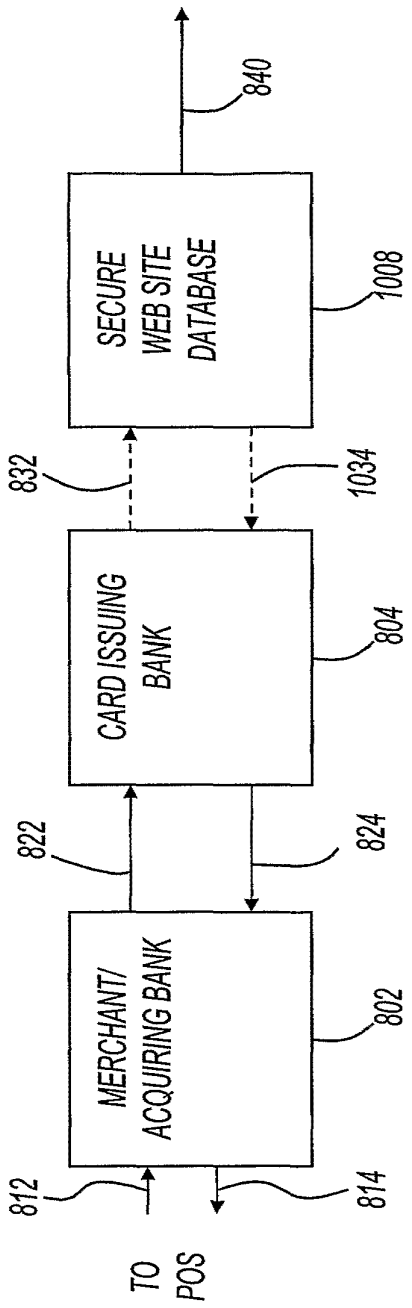

840
SECURE WEB SITE DATABASE
1008
832
1034
CARD ISSUING BANK
804
822
824
MERCHANT/ ACQUIRING BANK
802
812
814
TO POS

FIG. 10

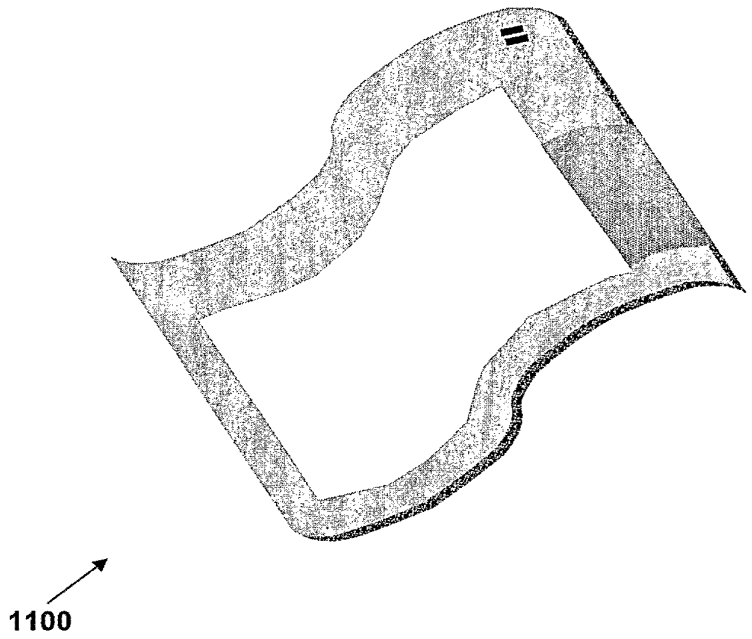


Fig. 11

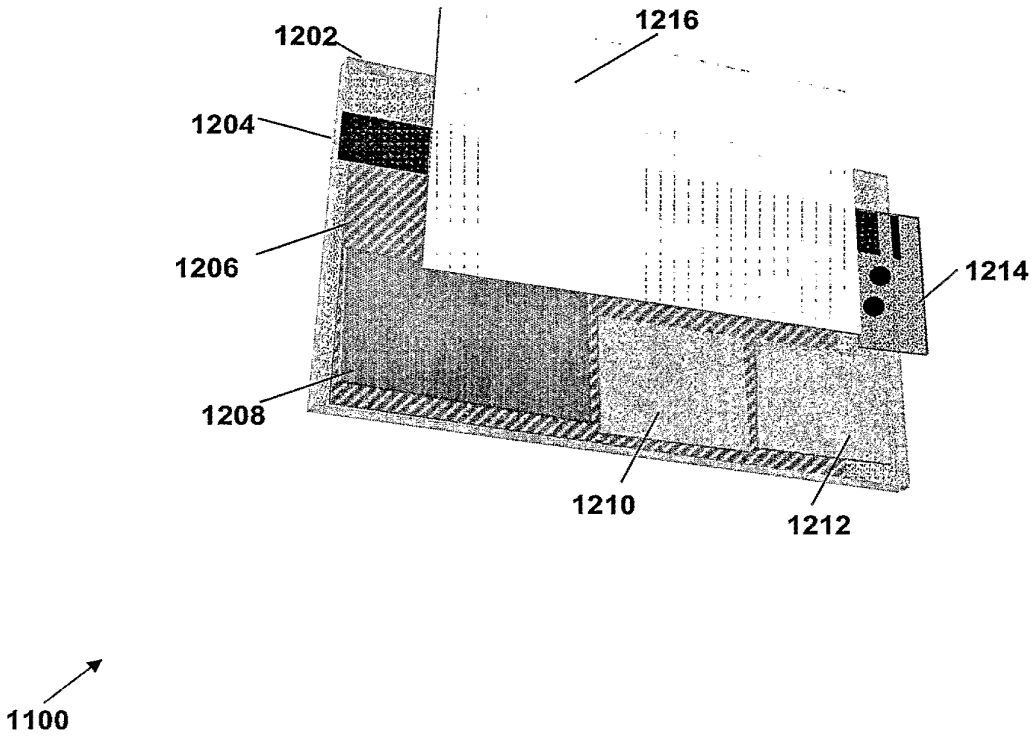


Fig. 12

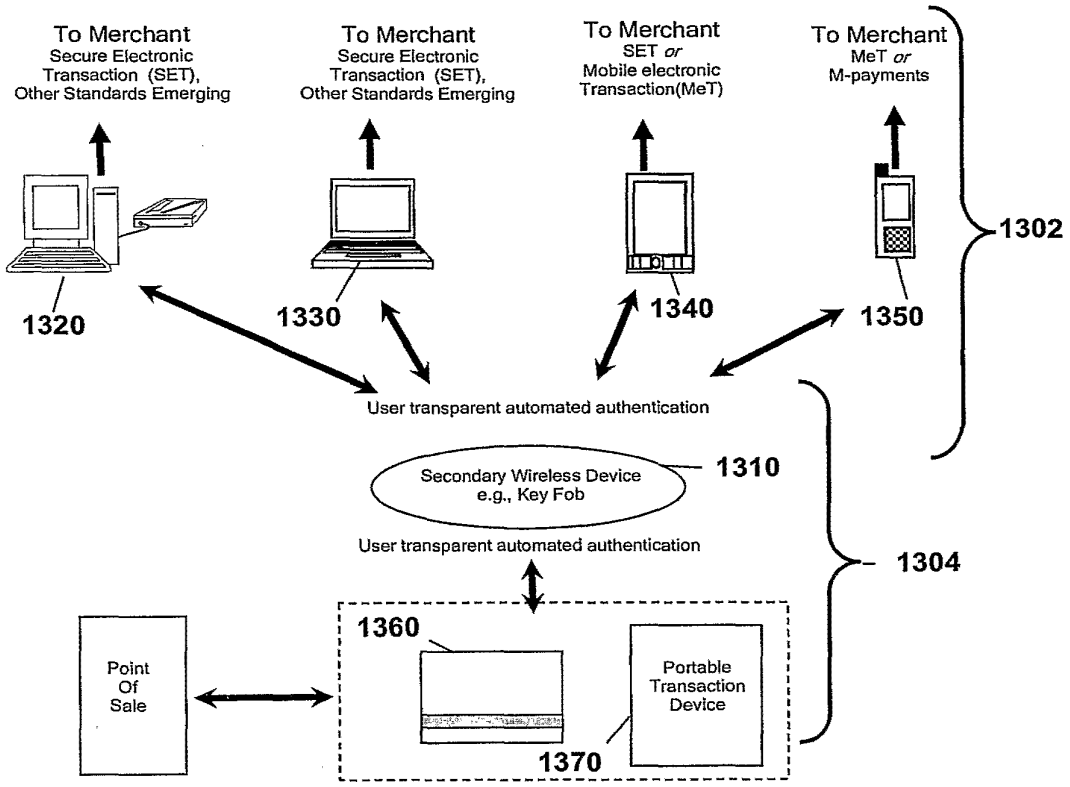

To Merchant
Secure Electronic Transaction (SET), Other Standards Emerging
To Merchant
Secure Electronic Transaction (SET), Other Standards Emerging
To Merchant
SET or Mobile electronic Transaction(MeT)
To Merchant
MeT or M-payments
1320
1330
1340
1350
1302
User transparent automated authentication
Secondary Wireless Device e.g., Key Fob
1310
User transparent automated authentication
1304
Point Of Sale
1360
Portable Transaction Device
1370

Fig. 13

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US2005/022993

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G07F19/00 G07F7/10

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 G07F

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 6 016 476 A (MAES ET AL) 18 January 2000 (2000-01-18)	1,2,4
Y	column 2, line 21 - column 4, line 22 column 4, line 65 - column 15, line 25 figures	3,5-20
Y	EP 1 291 748 A (ALCATEL) 12 March 2003 (2003-03-12) abstract column 2, paragraph 6 - column 4, paragraph 13 figure 1	3,5-20
X	US 2003/220876 A1 (BURGER TODD O ET AL) 27 November 2003 (2003-11-27)	1,2,4
A	page 5, paragraph 93 - page 22, paragraph 313 figures 1-11	3,5-20

-/--

[X] Further documents are listed in the continuation of box C.

[X] 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	Date of mailing of the international search report
12 October 2005	21/10/2005

Name and mailing address of the ISA	Authorized officer
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	Rachkov, V

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US2005/022993

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 2003/080183 A1 (RAJASEKARAN SANGUTHEVAR ET AL) 1 May 2003 (2003-05-01) page 1, paragraph 2 - page 3, paragraph 19 page 3, paragraph 35 - page 4, paragraph 41 figures 4,5	5-7
A	EP 1 161 060 A (NTT DOCOMO, INC) 5 December 2001 (2001-12-05) column 3, paragraph 7 - column 6, paragraph 23 figures 1-3	1,11-14, 17-19

Form PCT/ISA/210 (continuation of second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US2005/022993

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 6016476 A	18-01-2000	CZ 20000470 A3	17-03-2004
		DE 69828291 D1	27-01-2005
		EP 1004099 A1	31-05-2000
		WO 9908238 A1	18-02-1999
		HU 0004470 A2	28-05-2001
		IL 130068 A	12-01-2003
		JP 3476189 B2	10-12-2003
		JP 2001512876 T	28-08-2001
		PL 338353 A1	23-10-2000
EP 1291748 A	12-03-2003	US 2003048174 A1	13-03-2003
US 2003220876 A1	27-11-2003	NONE	
US 2003080183 A1	01-05-2003	WO 03038719 A1	08-05-2003
EP 1161060 A	05-12-2001	AU 771857 B2	01-04-2004
		AU 1732901 A	18-06-2001
		BR 0009958 A	27-04-2004
		CA 2356371 A1	14-06-2001
		CN 1340267 A	13-03-2002
		CN 1620175 A	25-05-2005
		HU 0200051 A2	29-04-2002
		WO 0143404 A1	14-06-2001
		NO 20013734 A	30-07-2001
		PL 349257 A1	01-07-2002
		TW 479187 B	11-03-2002
		US 6910624 B1	28-06-2005

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 August 2006 (31.08.2006)

PCT

(10) International Publication Number
WO 2006/091709 A3

(51) International Patent Classification:
G06K 19/073 (2006.01)

(21) International Application Number:
PCT/US2006/006361

(22) International Filing Date:
21 February 2006 (21.02.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/063,291 22 February 2005 (22.02.2005) US

(71) Applicant *(for all designated States except US)*: **TYFONE, INC.** [US/US]; 5520 SW Macadam Ave., Suite 250, Portland, OR 97219 (US).

(72) Inventors; and

(75) Inventors/Applicants *(for US only)*: **NARENDRA, Siva, G.** [IN/US]; 7180 SW 84th Ave, Portland, Oregon 97223 (US). **SPITZER, Thomas, N.** [US/US]; 1490 Clifton Street, Portland, Oregon 97201 (US). **TADEPALLI, Prabhakar** [US/IN]; 290 Phase II, Adarsh Palm Meadows, Airport Whitefield Road, Bangalore 560 066, Karnataka (US).

(74) Agent: **LEMOINE, Dana, B.**; Lemoine Patent Services, c/o PortfolioIP, P.O. Box 52050, Mineapolis, Minnesota 55402 (US).

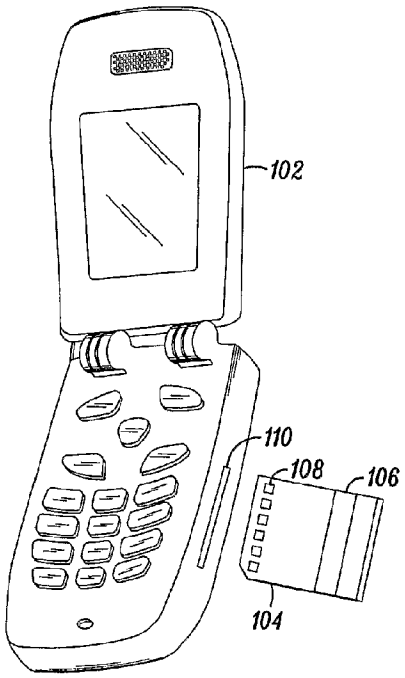
(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, 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, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, 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).

Published:
— *with international search report*

[Continued on next page]

(54) Title: ELECTRONIC TRANSACTION CARD



(57) Abstract: An electronic transaction card communicates with an add-on slot of an intelligent electronic device. The add-on slot may be a memory card slot. The intelligent electronic device may be a mobile phone or other device with or without network connectivity. The electronic transaction card may have magnetic field producing circuitry compatible with magnetic card readers, smartcard circuitry, other point-of-sale interfaces, or any combination thereof.

WO 2006/091709 A3

(88) Date of publication of the international search report:
21 December 2006

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.

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2006/006361

A. CLASSIFICATION OF SUBJECT MATTER
INV. G06K19/073

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)
G06Q G06K G07C

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	GB 2 316 908 A (JOHN * COWLING) 11 March 1998 (1998-03-11) page 2, paragraph 2 - page 5, paragraph 4; figure 1	1
Y		2-8, 11-14, 19,20
A	US 2004/087339 A1 (GOLDTHWAITE SCOTT ET AL) 6 May 2004 (2004-05-06) abstract	1-8, 15-20
A	US 6 721 196 B1 (GRASSL THOMAS) 13 April 2004 (2004-04-13) abstract	1-8,19, 20

-/--

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 September 2006	22/09/2006

Name and mailing address of the ISA/	Authorized officer
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	Beatty, John

1

Form PCT/ISA/210 (second sheet) (April 2005)

IPR2025-00644 Page 01184

INTERNATIONAL SEARCH REPORT

International application No
PCT/US2006/006361

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 96/26500 A (PEEK, GARRY) 29 August 1996 (1996-08-29) page 6, line 7 - page 10, line 18	9,10,15, 17
Y	the whole document	2-8, 11-14, 19,20

1

Form PCT/ISA/210 (continuation of second sheet) (April 2005)

IPR2025-00644 Page 01185

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No
PCT/US2006/006361

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
GB 2316908 A	11-03-1998	NONE	
US 2004087339 A1	06-05-2004	AU 2003288963 A1	07-06-2004
		EP 1563697 A2	17-08-2005
		WO 2004043048 A2	21-05-2004
US 6721196 B1	13-04-2004	AT 239296 T	15-05-2003
		AU 5683500 A	31-01-2001
		BR 0011868 A	09-04-2002
		CA 2377175 A1	04-01-2001
		CN 1358315 A	10-07-2002
		DE 19928733 A1	04-01-2001
		WO 0101418 A1	04-01-2001
		EP 1198797 A1	24-04-2002
		ES 2193968 T3	16-11-2003
		JP 2003503834 T	28-01-2003
WO 9626500 A	29-08-1996	AU 4498296 A	11-09-1996

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
31 August 2006 (31.08.2006)

PCT

(10) International Publication Number
WO 2006/091709 A2

(51) International Patent Classification: Not classified

(21) International Application Number:
PCT/US2006/006361

(22) International Filing Date:
21 February 2006 (21.02.2006)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/063,291 22 February 2005 (22.02.2005) US

(71) Applicant *(for all designated States except US)*: **TYFONE, INC.** [US/US]; 1490 Clifton Street, Portland, Oregon 97201 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: **NARENDRA, Siva, G.** [IN/US]; 7180 SW 84th Ave, Portland, Oregon 97223 (US). **SPITZER, Thomas, N.** [US/US]; 1490 Clifton Street, Portland, Oregon 97201 (US). **TADEPALLI, Prabhakar** [US/IN]; 290 Phase II, Adarsh Palm Meadows, Airport Whitefield Road, Bangalore 560 066, Karnataka (US).

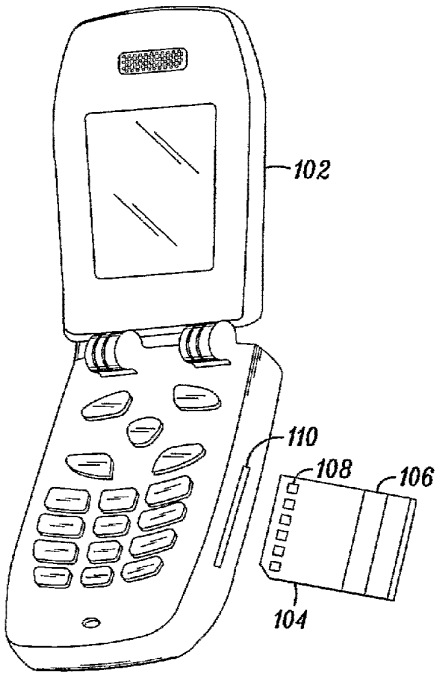
(74) Agent: **LEMOINE, Dana, B.**; Lemoine Patent Services, c/o PortfolioIP, P.O. Box 52050, Mineapolis, Minnesota 55402 (US).

(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, KE, KG, KM, KN, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, LY, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SM, SY, TJ, 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, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, 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).

[Continued on next page]

(54) Title: ELECTRONIC TRANSACTION CARD



(57) Abstract: An electronic transaction card communicates with an add-on slot of an intelligent electronic device. The add-on slot may be a memory card slot. The intelligent electronic device may be a mobile phone or other device with or without network connectivity. The electronic transaction card may have magnetic field producing circuitry compatible with magnetic card readers, smartcard circuitry, other point-of-sale interfaces, or any combination thereof.

WO 2006/091709 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.

ELECTRONIC TRANSACTION CARD

Field

The present invention relates generally to electronic devices, and more specifically to electronic devices that may perform transactions.

Background

Magnetic cards have many purposes. Examples include credit cards, debit cards, stored value cards, identification cards, access entry cards, and the like. Many of these cards have information stored in a magnetic stripe in a static manner. For example, a credit card may have a credit card number, a cardholder's name, and an issuing bank's name statically encoded in a magnetic strip. Likewise, an identification card or access entry card may have statically encoded information that identifies an individual or allows access to a controlled access area. When the card is swiped through a magnetic card reader, the information is transferred to the magnetic card reader to perform a transaction, such as a financial transaction or identification transaction.

Brief Description of the Drawings

Figures 1, 2A, and 2B show intelligent electronic devices and electronic transaction cards;

Figure 3 shows a block diagram of an electronic transaction card;

Figure 4 shows an electronic transaction card in a magnetic card reader;

Figure 5 shows an intelligent electronic device and card in a card reader;

Figures 6-8 show adapters for use with electronic transaction cards;

Figures 9 and 10 show an electronic transaction card having a smartcard interface;

Figure 11 shows an adapter in combination with an electronic transaction card;

Figure 12 shows an adapter having an aperture to receive an electronic transaction card;

Figure 13 shows another adapter embodiment;

Figure 14 shows an electronic transaction card;

Figure 15 shows an electronic transaction card and adapter combination;

Figure 16 shows an example swallow-type card reader;

Figure 17 shows a combination electronic transaction card and adapter being swiped through a magnetic card reader;

Figure 18 shows a financial transaction card;

Figure 19 shows a memory card;

Figure 20 shows a block diagram of a combination memory card and electronic transaction card;

Figure 21 shows a diagram of how a card may be utilized;

Figure 22 shows a block diagram of a combination memory card and electronic transaction card; and

Figure 23 shows a block diagram of a phone and a card.

Description of Embodiments

In the following detailed description, reference is made to the accompanying drawings that show, by way of illustration, various embodiments of an invention. These embodiments are described in sufficient detail to enable those skilled in the art to practice the invention. It is to be understood that the various embodiments of the invention, although different, are not necessarily mutually exclusive. For example, a particular feature, structure, or characteristic described in connection with one embodiment may be implemented within other embodiments without departing from the spirit and scope of the invention. In addition, it is to be understood that the location or arrangement of individual elements within each disclosed embodiment may be modified without departing from the spirit and scope of the invention. The following detailed description is, therefore, not to be taken in a limiting sense, and the scope of the present invention is defined only by the

appended claims, appropriately interpreted, along with the full range of equivalents to which the claims are entitled. In the drawings, like numerals refer to the same or similar functionality throughout the several views.

Figure 1 shows an intelligent electronic device and an electronic transaction card. Intelligent electronic device 102 is shown as a mobile phone in Figure 1, but this is not a limitation of the present invention. For example, intelligent electronic device 102 may be a personal digital assistant (PDA), a smartphone, a mobile phone, a handheld computer, or any other device capable of operating as described herein.

Intelligent electronic device 102 includes add-on slot 110. Add-on slot 110 is a slot capable of accepting electronic transaction card 104. For example, add-on slot 110 may have physical dimensions compatible with electronic transaction card 104, and may have a communications interface that operates using a protocol compatible with electronic transaction card 104. In some embodiments, electronic transaction card 104 includes an identification number that provides a relationship to intelligent electronic device 102. For example, electronic transaction card 104 may include an ID number that provides a unique pairing relationship or a non-unique pairing relationship between electronic transaction card 104 and intelligent electronic device 102.

In some embodiments of the present invention, add-on slot 110 is a memory card slot designed to accept and communicate with memory cards. As used herein, the term "memory card slot" refers to any add-on slot capable of accepting a card having memory accessible by an intelligent electronic device such as that shown in Figure 1. For example, a memory card slot may be a proprietary card slot designed to accept memory cards that adhere to a proprietary communications protocol. Also for example, a memory card slot may be compatible with an industry standard communications protocol, or may be compatible with a widely accepted communications protocol that is not necessarily formally documented as an industry standard. Examples include slots that are compatible with the Multimedia Memory Card (MMC) protocol, Memory Stick DUO protocol, secure digital (SD) protocol,

and Smart Media protocol. The foregoing list is meant to be exemplary, and not exhaustive. Add-on slot 110 may be compatible with many memory card slot protocols other than those explicitly listed above without departing from the scope of the invention.

Electronic transaction card 104 includes electrical contacts 108 and stripe 106. Electrical contacts 108 are contacts that provide a communications interface to communicate with add-on slot 110. For example, electrical contacts 108 may provide connectivity compliant with a communications protocol for memory cards.

Stripe 106 represents an area on an external face of electronic transaction card 104 at which one ore more time-varying magnetic fields emanate. For example, one or more time-varying magnetic fields may emanate from the location of stripe 106 to communicate with a magnetic card reader. In some embodiments, the time-varying magnetic field may emulate the time-varying magnetic field produced when a typical magnetic card is swiped through a magnetic card reader. For example, a time-varying magnetic field produced at stripe 106 may emulate the swipe of a credit card, a debit card, or any other card having a magnetic stripe compatible with a magnetic card reader.

In some embodiments of the present invention, stripe 106 may be a visible stripe on electronic transaction card 104. When stripe 106 is visible, it may be used to indicate the location at which the time-varying magnetic field will emanate. In other embodiments of the present invention, stripe 106 may not be visible. For example, circuitry may be included within electronic transaction card 106 to produce the time-varying magnetic field and no visible indication may be present on an external face of electronic transaction card 104.

As used herein, the term "stripe" generally refers to a location on an electronic transaction card, whether a visible stripe exists or not. In this description, the term "stripe" may also be used to refer to a visible marking on a face of an electronic transaction card. Further, a "stripe" may include the functionality provided by one or more time-varying magnetic fields that emanate from the card.

For example, the term "stripe" may refer to multiple magnetic tracks, or multiple "stripes," or emulation thereof.

Stripes, as described herein, may be compatible with one or more standards. A stripe may be compatible with a standard by being in compliance with the standard or by being partially in compliance with the standard. For example, stripe 106 may be compatible with an American National Standards Institute (ANSI) magnetic stripe standard, or an International Organization for Standardization (ISO) magnetic stripe standard. In addition, in some embodiments, a stripe may emulate more than one magnetic track, and the emulated tracks may or may not be offset from the location specified in a standard. For example, one or more wires may be utilized to generate time-varying magnetic fields compatible with a standard, and the wires may be located at or near stripe 106 in a location different than the magnetic track offset described in an associated standard.

As used herein, the term "transaction" refers to any beneficial use of an electronic transaction card. For example, any time stripe 106 emits a time-varying magnetic field to be read by a magnetic card reader or a hybrid smartcard reader, a transaction may take place. Transactions may include financial transactions, access control transactions, or any other type of transaction involving any of the electronic transaction card embodiments described herein. Further, as described in more detail below, in some embodiments of the present invention, transactions may utilize smartcard interfaces on electronic transaction cards in addition to, or in lieu of, stripes that emit time-varying magnetic fields.

In operation, intelligent electronic device 102 may program electronic transaction card 104 for use in a transaction involving stripe 106. For example, intelligent electronic device 102 may program electronic transaction card 104 to operate as a credit card, a debit card, or the like. Electronic transaction card 104 may then be used with a magnetic stripe or smartcard based merchant point-of-sale terminal to effect a transaction. Also for example, intelligent electronic device 102 may program electronic transaction card 104 to operate in any other environment where stripe 106 may be beneficially utilized with a magnetic card reader.

Figure 2A shows intelligent electronic device 202 and electronic transaction card 220. Intelligent electronic device 202 includes add-on slot 210 to receive electronic transaction card 220. Intelligent electronic device 202 is shown having add-on slot on one side, but this is not a limitation of the present invention. For example, add-on slot 210 may be located on top, bottom, or any other surface of intelligent electronic device 202. Also for example, an add-on slot may be created by a clamshell design when the shell is closed. In these embodiments, each side of the clamshell may incorporate a portion of the add-on slot such that the add-on slot is "open" when the clamshell is open.

Electronic transaction card 220 may have any form factor compliant with add-on slot 210. Electronic transaction card 220 is shown having a form factor with an aspect ratio different from that of electronic transaction card 104 (Figure 1). Electronic transaction card 220 includes stripe 222 and may have electrical contacts to interface with add-on slot 210. The electrical contacts may be on the back side of electronic transaction card 220, recessed on an edge of electronic transaction card 220, or on the front side of electronic transaction card 220. In some embodiments, electronic transaction card 220 includes a "contactless" interface to add-on slot 210. For example, electronic transaction card 220 may include an interface to add-on slot 210 that communicates using electric or magnetic fields, infrared (IR) light, or any other suitable communications mechanism.

Electronic transaction card 220 may have an area for imprinting. For example, as shown in Figure 2A, electronic transaction card 220 may have space for imprinting a brand (for a bank or otherwise), and a cardholder's name. Further, electronic transaction card 220 may include space for a cardholder's signature. Electronic transaction card 220 may include any other information, coded or unencoded, visible or nonvisible, without departing from the scope of the present invention.

Intelligent electronic device 202 may include a mechanism to allow intelligent electronic device 202 to communicate with a wired or wireless network. For example, intelligent electronic device 202 may include circuitry to communicate

with a cellular phone network. Note that in these embodiments, intelligent electronic device 202 may or may not be a phone. For example, intelligent electronic device 202 may be a cellular telephone with an add-on slot for use with an electronic transaction card. Also for example, intelligent electronic device may be a non-telephonic device that has cellular network connectivity. Examples include personal digital assistants, and handheld devices dedicated to the use of electronic transaction cards. Further, intelligent electronic device 202 may be a non-telephonic device having wired or wireless connectivity to a network other than a cellular network, and in some embodiments, intelligent electronic device 202 may be a device without network connectivity. Examples include, but are not limited to: Blackberry devices available from Research in Motion (RIM), music players such as MP3 players, cameras, and the like.

In operation, intelligent electronic device 202 may program electronic transaction card to perform a transaction. In some embodiments, communications over a network may play a role in the transaction. For example, intelligent electronic device 202 may receive authorization for the transaction over a network. Also for example, intelligent electronic device 202 may program electronic transaction card 220 to perform a transaction, and then report the transaction to an entity using the network.

Electronic transaction card 220 may be utilized in financial transactions. For example, electronic transaction card 220 may be programmed to operate as a credit card or a stored value card. In these embodiments, electronic transaction card 220 may be programmed to emit one or more time-varying magnetic fields to emulate the swiping of a credit card or stored value card. In some of these embodiments, electronic transaction card 220 may use one number repeatedly, or may use a different number for each transaction. For example, electronic transaction card 220 may be programmed to have one number, similar to how a credit card uses the same number repeatedly. Also for example, electronic transaction card 220 may be programmed to use a different number for each transaction. These numbers are referred to herein as "single transaction account numbers" or "STANs."