METHOD FOR REPLACING TRADITIONAL PAYMENT AND IDENTITY MANAGEMENT SYSTEMS AND COMPONENTS TO PROVIDE ADDITIONAL SECURITY AND A SYSTEM IMPLEMENTING SAID METHOD

Inventors: Charles David Tunnell, Palm Bay, FL (US); Justin Mitchell, Melbourne, FL (US); Gino Pereira, Oxford, CT (US); Jacob Zurasky, Orlando, FL (US)

Assignee: NXT-ID, Inc., Shelton, CT (US)

Filed: Oct. 8, 2013

Publication Classification

Int. Cl. G06Q 20/36 (2006.01)
U.S. Cl. G06Q 20/363 (2013.01)
CPC G06Q 20/363 (2013.01)
USPC 708/41

ABSTRACT

An electronic wallet system that protects payment accounts, identification and other personal information found within a typical wallet with a secure electronic vault (first) device that can be part of a physical wallet, insert to a wallet, or in other embodiments, wearable/ portable devices. A unique biometrically enabled multi-factor authentication process ensures only owners of the information can copy the information to the device or retrieve it thereafter. Authenticated users may then select payment, identification, medical or virtually any private information via touch display or voice command on the vault or on another (second) device that operates in conjunction with the vault. The second device comprises, for example, a programmable card with dynamic magnetic stripe, cell phone, or other wearable technology, that initiates and processes a payment and/or transfer of private information.
Figure 3

Figure 4
Figure 11

- **Second Devices (Display)**
  - Dynamic pairing or equivalent
  - Cell phones, tablets, laptops, PCs & the like

- **Personal Identity Vault**
  - Dynamic pairing or equivalent
  - Part of physical wallet, insert, or wearable/portable device

- **Second Devices (Comms)**
  - Dynamic pairing or equivalent
  - Powered cards, cell phones, tablets, laptops, PCs & the like
METHOD FOR REPLACING TRADITIONAL PAYMENT AND IDENTITY MANAGEMENT SYSTEMS AND COMPONENTS TO PROVIDE ADDITIONAL SECURITY AND A SYSTEM IMPLEMENTING SAID METHOD

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This patent application claims the benefit of the U.S. provisional patent application filed on Oct. 8, 2012 and assigned Application No. 61/710,826, which is incorporated herein.

FIELD OF THE INVENTION

[0002] The present invention relates to the field of digital and electronic wallets, specifically methods and related apparatuses for securing private information found within a typical wallet, such as payment accounts, payment cards, identification information, medical information and records, and virtually any private information desired to be carried by a person.

BACKGROUND OF THE INVENTION

[0003] Prior art digital wallets focus on financial transactions, attempting to replace current technologies of credit and debit cards and the like with mostly electronic commerce (e-commerce) and similar methods and devices. Likewise, security concerns for most digital wallet technologies are focused primarily on the transaction between the customer, merchant and banking institutions.

[0004] The term “digital wallet” is used loosely to describe a broad spectrum of methods and devices to perform electronic commerce (e-commerce). Digital wallets refer to software that resides on the consumer’s personal computer (PC) or other web-enabled devices that enable a user to select a payment account digitally. Digital wallets require an internet connection. Conversely, electronic wallets refer to electronic methods to allow a user to select a payment account locally, on some physical electronic device. Most digital wallet technologies involve software that resides on the consumer’s personal computer (PC) or other web-enabled devices. Most browsers now support digital wallets. Digital wallet software spans methods to improve consumer’s ability to purchase goods and services from on-line e-retailers (the “transaction”) to methods to keep personal information private (the “security”).

[0005] Features and benefits to the consumer to purchase goods and services over internet based e-commerce are well known. However, many shortcomings have limited the use and acceptance of digital wallet software solutions as the technology migrates to mobile devices. The chief issue with mass consumer acceptance of “mobile money” solutions involves securing private information on the devices as well as securing authentication information during the transaction itself. As evident in recent reviews, digital wallet technologies on cell phones will be further challenged to fully secure mobile devices. Security holes within operating systems and firewalls have caused numerous false starts to an already skeptical consumer market. Even if security concerns can be overcome, the perception of the public to utilize cell phones that have open access via the internet is questionable. In this day of rampant identity theft, consumers are understandably cautious to embrace any technology that houses or transmits their private information over electronic mediums without “assured security.”

[0006] Various methods have been used to secure financial transactions over the internet including encrypting the information stored locally on a device as well as the information transmitted to merchants and on to banking institutions. Since encryption alone does not solve the issue of authenticating, that is, is the individual making the purchase is indeed the individual qualified to make the purchase (e.g. the “card holder”), various methods to “authenticate” the user have arisen, such as biometrics. “End-to-end” biometric authentication is great for a long-term solution (once all security issues are fully addressed to the satisfaction of consumers), but does nothing for the current paradigm of magnetic stripe credit and payment cards that are so prevalent in society. Furthermore, a simple biometric key that authenticates with a server in the cloud does nothing to address hacking of the device and using the captured bio-key improperly “remotely” over the internet.

SUMMARY OF THE INVENTION

[0007] One embodiment of the invention comprises a method to send private information to authenticated devices securely to replicate the information in a format that supports a specific transaction method, and thereby reduce the number of devices, cards and other methods a user must carry, while improving security to protect private information.

[0008] The invention also addresses the broader issue of securing and replacing the number and variety of devices holding personal information within a wallet, such as identification information, medical information, and payment account devices, while conforming to current transaction methods, such as those utilizing magnetic stripes and/or NFC (near-field communications) for financial transactions and other known methods for HIPPA-controlled medical documents.

[0009] One embodiment of the invention focuses on security between a secure electronic payment and identity management device (referred to as a first device) and second devices that facilitate a transaction per a conventional transaction method, such as a dynamically programmable card and/or a mobile device such as a cell phone. This dual device relationship arguably addresses where most theft and fraud occurs, prior to the point-of-sale (POS), replacing payment transaction accounts and other private information with one or more standard devices that can perform the transaction over standard communications, only after being authorized to receive the private information from the first device, such as a private electronic vault or an electronic wallet. Unlike current methods that hold and transfer information (such as payment cards and other devices that support USB (universal serial bus), infrared, magnetic stripe, NFC (near field communications), contact/contactless EMV (Europay, MasterCard and Visa)), this invention requires a second device to authenticate with the secure electronic payment and identity management device before a transaction can occur, even if the information is transferred via one of these communication methods directly to a POS terminal directly from the private electronic wallet or via an authenticated second device. Thus, the second device can be “dumb” most of the time, completely void of any personal information, while the private electronic wallet
device holds all private data safe and secure, and only releases it to secondary device(s) or POS terminals after a full authentication has occurred.

The present invention provides unique alternatives to reducing the number and variety of devices holding personal information within a wallet while increasing security of the user authentication process and the consumer transaction. To conform to current payment methods, rather than requiring any special software or equipment modifications by a merchant or bank, this invention reduces the number of payment devices and methods carried by a user and increases security while working within the paradigm of the current magnetic stripe readers, contactless NFC and EMV systems, and bar code payment methods that are so prevalent within society today. Further, this invention addresses chief security concerns not only with physical electronic wallets, but also digital wallets on mobile devices such as cell phones, which desperately need authentication and security solutions to overcome current mobile payment security deficiencies and user perceptions.

This invention improves security by requiring authentication between a user and two devices (i.e., the first and second devices) primary to any transaction taking place. The first device is an electronic vault device that can be physically part of a physical wallet, insert to a wallet, or in other embodiments, wearable/portable devices such as money clips, key chain accessories, watches, dongs, cell phone accessories, or any other device typically carried or worn by an individual. The first device requires unique user-configurable, biometrically enabled multi-factor authentication to ensure only owners and their private information can be copied into the secure vault wallet device.Authenticated users may then select payment information, identification information, medical information or virtually any private information via touch display or voice command on the first device, or alternatively on the second device after a successful authentication.

Encrypted information can be sent from the first device to the second device, after successful authentication. The second device can comprise a programmable card having a dynamic magnetic stripe, a cell phone, or a display device displaying a payment barcode to replicate the selected private information stored on the first device. This method and attendant devices reduces the number of cards and other devices a user must carry. The second device may include mobile devices such as cell phone, tablets and laptops, or fixed devices such as desktop PCs and the like. The second device then acts as a conduit to provide private information via other communication methods such as NFC or dynamic magnetic stripe for financial transactions, and HIPAA controlled communication methods for private medical documents.

BRIEF DESCRIPTION OF THE DRAWINGS

The foregoing and other features of the present inventions will be apparent to one skilled in the art to which the present inventions relate upon consideration of the following description of the invention with reference to the accompanying drawings, herein:

FIG. 1 is a conceptual drawing of the private electronic vault with secondary authenticated device, in this case a powered card.

FIG. 2 is a mechanical design of the invention configured with the display of the private identity vault device on the outside of the wallet.

FIG. 3 illustrates mechanical designs with the display located at the left 115 or the right 116 sides of the inside of the wallet.

FIG. 4 is a mechanical design of the personal identity wallet as an insert 117 to a conventional wallet.

FIG. 5 is a mechanical design of a standalone personal identity vault with an optional clip for inserting into a conventional wallet.

FIG. 6 describes another embodiment of the mechanical design of this invention to not only hold a powered card, but also communicate with it and charge its battery by aligning physical contacts or embedded electrical components such as antenna, coils, or the like.

FIG. 7 is a mechanical design of a standalone private electronic wallet with optional enclosed card.

FIG. 8 is a mechanical design of a standalone private electronic vault with an optional open card and clip for insertion into a conventional wallet.

FIG. 9 is a mechanical design of a standalone private electronic vault with an optional open card and clip for insertion into a conventional wallet.

FIG. 10 is a mechanical design of a clamshell wallet with private electronic vault embedded in the wallet (part of the wallet) with an optional enclosed card.

FIG. 11 describes an authentication process called dynamic pairing that can authenticate between a personal identity vault and a secondary device acting as a controller and display for the vault, and another second device acting as a conduit to support consumer transactions via communication paths not inherent on the personal identity vault.

FIG. 12 is a block diagram of the personal identity vault that illustrates the major functional blocks of the invention.

FIG. 13 is a block diagram of a powered card as a secondary device with major functional blocks of the invention including a dynamic magnetic stripe module.

FIG. 14 describes areas where pinch conductive material can be applied to both sides of a powered card to achieve pinch power, a method to turn on a powered card by completing a circuit as a user naturally holds the card.

FIG. 15 illustrates a pinch power prototype with copper material on the designated areas of both sides of a card and an LED that lights to show when the card is pick up, the circuit activates the powered card.

FIG. 16 illustrates a pinch power prototype with transparent conductive material on designated areas of both sides of a card.

FIG. 17 details how two devices authenticate one another via dynamic pairing.

FIG. 18 describes a user interface (UI) concept for a user to access a private electronic vault by drawing a user-configured pattern.

FIG. 19 describes a user interface (UI) concept for a user to access a private electronic vault by typing a user-configured PIN.

FIG. 20 describes the user interface (UI) for the private electronic vault where users may select from user-configured aliases.

FIG. 21 describes the user interface (UI) for scrolling through user-definable categories on the private electronic vault.

FIG. 22 describes another user interface (UI) concept for a user to access categories of aliases to personal information.
FIG. 23 describes another user interface (UI) concept for a user to access preferred aliases.

FIG. 24 describes a user interface (UI) concept for a user to view details of private information such as a payment card.

FIG. 25 describes another user interface (UI) concept for a user to view details of private information such as a payment card.

FIG. 26 describes a user interface (UI) concept to manage personal information and cards within a private electronic wallet from an app on a second device, such as mobile and fixed devices like cell phones, tablets, laptops, PCs and the like.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS

Before describing in detail the particular methods and apparatuses related to replacing traditional payment and identify management systems and components with methods and components that provide additional levels of security, it should be observed that the embodiments of the present invention reside primarily in a novel and non-obvious combination of elements and method steps. So as not to obscure the disclosure with details that will be readily apparent to those skilled in the art, certain conventional elements and steps have been presented with lesser detail, while the drawings and the specification describe in greater detail other elements and steps pertinent to understanding the embodiments. The presented embodiments are not intended to define limits as to the structures, elements or methods of the inventions, but only to provide exemplary constructions. The embodiments are permissive rather than mandatory and illustrative rather than exhaustive.

The present invention differs from other “digital wallets” in that other wallets are more focused on solutions that rely upon an internet connection to perform card/account selection and/or transaction. In contrast, this invention is focused on replacing the number and variety of devices holding personal information within a physical wallet, and replicating their functionality onto a secondary authenticated device that conforms to current common communication interfaces for private methods such as HIPPA controlled communication methods for private medical documents and payment methods such as NFC or dynamic magnetic stripe.

System Overview

This invention improves security by requiring authentication between a user and two devices as shown for example in FIG. 1 (referred to herein as first and second devices) prior to a transaction taking place. The first device, which may comprise and be referred to as an electronic vault device, personal identity vault, private electronic vault, a private electronic wallet, a secure electronic payment and identity management device, a secure electronic payment and identification device or system, a next generation payment and personal identity wallet, and a next generation payment and personal identity device, can be physically part of a physical wallet as shown for examples in FIGS. 2 and 3, 102 and 104, insert to a wallet as shown in FIG. 4, 106, or in other embodiments, wearable/portable devices such as money clips, key chain accessories, watches, dongles, cell phone accessories, or any other device typically carried or worn by an individual. This personal identity vault device requires unique biometrically enabled multi-factor authentication to ensure only owners and their private information can be copied into the vault device.

Authenticated users may then select credit, debit, identification, medical or virtually any private information via touch display or voice command on the first device, or alternatively on the second device that connects to the first device. Encrypted information can be then sent from the first device to the second (authenticated) device, such as a programmable card with dynamic magnetic stripe. In any case, the format of the information in the second device is selected to replicate the desired transaction method. In one embodiment, for example, the second device can be pre-programmed to be any card type, such as a stand-alone multi-card, or the second device can sit within the electronic wallet device, which acts as a security system for programming the dynamic card. Information can be “zeroized”, writing 1’s and 0’s over memory iteratively in random pattern, after one use, a pre-configured number of uses, or after a timer has expired.

A user may select a card via the touch interface or voice command on the first device or alternatively on an authenticated second device with display interfaces (e.g. cell phone, tablet, PC, etc.), and configure the second device to function just like a copied device. Alternatively, the first device (e.g., private vault electronic wallet device) and the authenticated second device can be used with other mobile payment forms such as NFC, EMV, RFID, infrared, acoustic, and QR Codes in some embodiments. Logos, picture of the front and back, signature and even bar codes can be displayed on the sunlight readable display of the first or second devices such that secure electronic payment and identification system can uniquely support all common methods of payment currently supported at point of sale (POS) positions around the world. Other security methods such as a physical signature on the back of a payment device can also be supported.

Mechanical Options

The private electronic vault can encompass many embodiments spanning varying mechanical configurations. As shown in FIG. 1, one embodiment consists of a standalone private electronic vault 100 with secondary authenticated device, in this case a powered card 101 that can be located anywhere with the vault. FIG. 2 describes a mechanical design of the invention configured with the display of the private identity vault device embedded in the wallet and visible on the outside of the wallet. Features of this and any of the embodiments of this invention may include, as options, a display 102 that can be inserted into a wallet or embedded into an carried or worn device, a touch panel overlay 103, a battery indicator 104, a power on/off button 105, a microphone with exposure through the enclosure for appropriate acoustics 106, soft or hard material 107 appropriate for gripping the wallet and/or protecting other cards within the wallet such as blocking/attenuating signals to protect RF cards within, curved design 108 to conform to wearing in a rear or front pocket of a person’s clothing, magnetic clasps 109 that keeps the wallet closed until opened, magnetic switch 110 that turns the electronic wallet on and off as the wallet is opened, an area for a secondary device 111, a hinge or fold mechanism 112, areas and/or folds 113 for other cards and/or receipts, and/or a money clip 114.

Another embodiment of the mechanical design of this invention is to place the display inside the wallet. FIG. 3 illustrates this concept with the display located at the left 115 or the right 116 sides of the inside of the wallet.
Another embodiment of the mechanical design of
this invention is to provide the private electronic wallet as an
insert to a conventional wallet as shown in FIG. 4. FIG. 5
describes the enclosure of a standalone configuration that
stores the display and electronics of the private electronic
vault, alone with an attachment that serves as a dual
purpose as a storage method for a powered card and an
insert to hold the device in place inside a pocket of a
conventional wallet.

Another embodiment of the mechanical design of
this invention is to provide the private electronic wallet as an
insert to a conventional wallet as shown in FIG. 4. FIG. 5
describes the enclosure of a standalone configuration that
stores the display and electronics of the private electronic
vault, alone with an attachment that serves as a dual
purpose as a storage method for a powered card and an
insert to hold the device in place inside a pocket of a
conventional wallet.

Another embodiment of the mechanical design of
this invention described in FIG. 6 is to not only hold a card or
powered card with guide and ramp features, but also
communicate with a powered card and charge its battery by
aligning physical contacts or embedded electrical components
(not shown) such as antenna, coils, or the like.

Other embodiments include standalone private electronic
wallet 124 with optional enclosed card 125 using
molded guides as shown in FIG. 7, optional removable
insert as shown in FIG. 8, an open version of the private
electronic vault 128 where the molded guide is open 129 to
allow easier grip to a card, and a clip may be either molded
130 or removable 131. These standalone embodiments con-
tast to another clamshell design as shown in FIG. 10, but may
still possess each of the optional features such as a hard or soft
case, display 133, touch screen 134, modern design for
comfort such as tapered corners and sides 135, microphone
136, battery indicator 137, power button 138, magnetic clasp
139 and/or magnetic switch 140, hinge 141, card holders
142, and/or money clip (not shown on this drawing).

Electronic Hardware Components

As shown in FIG. 11, personal identity vaults 143
may communicate to multiple secondary devices 144 and 145
with NXT approved authentication such as dynamic pairing
146 or equivalent authentication methods. Some second
device 144 may act as a display for the personal ID vault,
while other second devices 145 act as a conduit to send private
information over other protocols and methods not inherent
to the vault.

The hardware for the private electronic vault and
one embodiment of a second device hardware may be similar
as shown in FIGS. 12 and 13, consisting of an ultra-low-power
microprocessor 147 powered by batteries or super-capacitors
148 managed by a battery monitor, input power condition, DC
to DC converters, recharging circuits with optional inductive
and/or RF wireless recharging circuits, all within a power
management block 149. The microprocessor 147 acts as the
microcontroller for all onboard peripherals including RAM
and NAND memory 150, or optionally FRAM and/or
NVRAM (shown as part of the memory block in the
diagram) in some configurations. For either of the
two devices, the microprocessor 147 may interface with an
optional low-power e-paper, memory LCD and/or color display
151. A transparent/semitransparent touch screen may be
overlaid atop the display 152, in some configurations, and
optionally wired directly to an analog comparator module
within the microprocessor for ultimate low power perfor-
mance while filtering and interpreting touch events, or
replaced with physical buttons (not shown) outside of the
display for user interface controls. The vault also contains a
multi-factor voice recognition algorithm via voice collected
by an onboard microphone that connects directly to dual stage
amplifiers within the processor for filtering and amplifying
the voice. Amplifiers within the processor further reduce
power consumption and chip count/cost. Both devices may
also communicate via contacts 123, USB 154 or optional
wireless communication including BTLE (Bluetooth Low
Energy) 155, NFC/EMV 156, RFID 157, infrared 158, optical
159, WiFi 160, acoustic 161, or custom low-power RF
communication (not shown). In addition to multi-factor
speaker and voice recognition (voice recognition), which
is inherent on an private electronic wallet device, other biometric
may be optionally added including gesture, finger, face,
3D face, IRIS, eye, eye vein, eye tracking, DNA, vein, palm,
heartbeat, sweat, vibrometry, and/or scent by adding those
sensors to the interface of the microprocessor. Microproces-
sors on each device may also integrate with a tamper-proof
authentication crypto chip 153, which houses identifiers, high
quality random number and key generators internally such
that no keys or identifiers are ever released by the authenti-
cation chip. Only random numbers are ever passed over
encrypted communicated between the first and second
devices.

The second device (or in those embodiments having
a plurality of second devices) may provide a conduit to trans-
fer the private information over some specific payment or
transaction methods that exist on the second device. For
instance, some commercial devices may support various
communication methods such as WiFi or NFC, negating the need for
the next generation payment and personal identity wallet to sup-
port these methods directly on its device. Instead, the private
electronic vault device (the first device) may simply commu-
nicate to the second device that then acts as a conduit to
adhere to any communication standards from authorities that
dictate the transfer of private information, such as HIPPA or
financial authorities.

The second device(s) may comprise any mobile,
portable, or wearable device such as cell phones, tablets and
the like, or even fixed computing devices such as PCs. In one
embodiment, as shown in FIG. 13, the second device can
contain similar components (in function), but not necessarily
such as the same chip as that with the primary electronic vault,
such as a crypto chip 153, ultra low-power processor 147,
flash memory, SDRAM, FRAM or NVRAM (collectively
part of the memory block of the diagram), display 151 and
touch screen 152, battery 148 and power management 149,
crypto 153, microphone 162, biometric modules 162 and
communications methods such as USB 154, BTLE 155,
NFC/EMV 156, RFID 157, infrared 158, optical 159, WiFi
160, acoustic 161, or custom low-power RF communication
(not shown). These second devices powered cards 165 may
also include a dynamic magnetic stripe module 164 to inter-
face with mag stripe card readers using a powered card. For
secondary powered cards specifically, each of the compo-
nents may be wired thinner versions of these chips, wafer or
die formats 0.5 mm or thinner, in order to conform to ISO
standards for payment cards of approximately 0.79 mm or
thinner). Displays on these cards may also be thinner and can
include other ultra thin displays that shows the payment account
number 166, in whole or in part, and other informa-
tion such as CVV 167, name 169 and expiration date 168 as
shown in FIG. 14.

Power Management: Battery and/or super-capacitors
(collectively shown as block 148) are continuously moni-
tored by power management 149 at a predetermined time
interval to activate a "low-battery" indicator (LED or equiva-
lent shown as part of the Power Management block 149) when
power is measured to be below a specific threshold. A
rechargeable circuit (shown as part of block 149) allows
Power to be recharged when connected to a 5 VDC USB device, or alternatively to be recharged via optional wireless inductive or RF charging methods, or other power harvesting methods such as solar/light, RF, piezoelectric/movement and thermal (each shown as part of the power management block 149 on the block diagram).

[0058] According to this invention, a second device, such as a dynamically programmable card, can be charged wirelessly by the private electronic vault (i.e., the first device) while the dynamically programmable card is near the private vault device, such as within a wallet. An optional wireless inductive ultra thin coil (shown as part of block 149) associated circuitry enables the primary device to communicate and charge the second device(s) using inductive charging conforming to the QI interface standard for inductive electrical power transfer. Alternatively, power may be transferred from the first or primary device to the secondary device via RF energy, such as BTLE, by adding an optional amplifier (shown as part of block 149) that boosts the RF energy on the primary device, and an optional power-harvesting chip (shown as part of block 149) on the Bluetooth transceiver on the secondary device. Under this scenario, a powered card sitting within a wallet can be charged by the electronic vault by sending information to the electronic vault when charging should take place. Thus, with this scheme, the battery within the powered card can be kept charged just as long as the larger battery for the private electronic vault (the first or primary device) within the wallet has charge, thereby extending the overall operation of the powered card (second device).

[0059] Power states are closely controlled within the microcontroller to achieve ultra lower power consumption and longest battery-life between charges. To take advantage of the infrequent use of a wallet in real-life, power may be totally turned off and turned back on using an innovative switch to FET (field effect transistor), which ensures no power is consumed when the device is powered off. Alternatively, to provide low power performance of the wallet while also automating the on/off mechanism, a magnetic switch 110 may be connected to a FET such that the electronic wallet automatically turns on as the wallet is opened, and off as the wallet is closed. The advantage of these two switch methods is that no power is consumed while the wallet is powered completely off; which increases the time between charging the battery.

[0060] When the private electronic vault is powered on, the microprocessor can be held at various “power states” that turn off the core processor and all peripherals except the a GPIO pin that can be used to wake up from “deep sleep”. Other power states include keeping the core off while interfaces to peripherals on. This enables DMA (direct memory access) transfers from one peripheral, such as memory, to another peripheral, such as the display, with minimum involvement (and power) by the processor. This allows the microprocessor to be kept at its lowest state and “wake-up” to other states only when the core processor is needed. This schema achieves lower power performance by “ping-ponging” between power states only as resources on the ultra low power microprocessor are needed. For instance, power can be conserved by waking up the microprocessor from its lowest power state (deep sleep) while it scans the touch screen at a very low frequency, increase to another state to capture the touch gesture by increasing frequency of scanning of the buttons, and returning to the lower power state after the touch has been completed. Likewise, interpreting the touch via table rather than requiring a processor to process the touch results can conserve power. Furthermore, power can be saved by transferring data via DMA to a display or RF peripheral that can then be awakened and display, process, or transmit that data. Thus, under this method, an event, such as a touch event, can be interpreted and data sent to a display and other peripherals while conserving power by ping-ponging the microprocessor between states.

[0061] Another unique power reduction feature is to power peripherals of the microcontroller directly from GPIO (general purpose input/output) pins such that any peripheral can be powered on or off directly by the microprocessor. With this schema, no current is consumed by any peripheral unless the microprocessor “wakes up” that peripheral by turning on the appropriate GPIO pin. Powering the peripherals directly by the microprocessor in this manner not only reduces needless power consumed while a peripheral is not used (e.g. in a quiescent state), but also reduces chip count by eliminating DC supplies.

[0062] To further reduce power, the secondary device can be awakened via a membrane switch, or optionally by an RF wake-up circuit or “pinch power” methods. The RF wake-up circuit consists of a resonantly tuned antenna with a receiver that then harvests the power from that signal to wake-up the rest of the circuit. Similar to semi-passive RFID, this RF wake-up method utilizes the frequency and power of the transmitter to create a resonant signal whose power can be harvested to wake-up the microprocessor. This method can be applied to Bluetooth Low Energy (BTLE), NFC, RFID or virtually any RF circuit.

[0063] Pinch Power: Another method to turn on and off powered cards is pinch power. As shown in FIG. 14, a card may remain in an “off state” until a user “pinches” both sides of the card, completing a circuit by shorting electrical conductive material 136 placed on both sides of the card. Most prior art for conserving energy on a powered card requires the user to actively take some action to activate the powered card, such as push a button in a certain area of the card or flip the card. An advantage of this pinch power method is that it utilizes no such user activity. The card simply works as the user naturally picks up the card.

[0064] Pinch power allows the device to be powered on by latching the power and can be turned off by the processor 147 when the card is done being used or a timeout occurs. A pinch power device is constructed by applying two planes of conductive material 170 to specific regions on opposite sides of the card as shown in FIG. 14. These regions are selected to avoid specific areas of the card, such as where a bar code 177 might be located or the magnetic strip 171 in FIGS. 14 and 178 in FIG. 15. When grasping a card in non-conductive areas 174 as shown by the prototype in FIG. 15, nothing happens as indicated by the non-lit LED 173 in this prototype. As a user grasps both sides of the card in the conductive regions of the card 175 (as one would naturally do when attempting to use the card), a conductive path is completed by the user’s fingers 175 and activates the Pinch Power latching circuit (not shown but described below), which in turn lights the LED 176 (for purposes of this prototype). Conductive regions 170 can be achieved either by exposing a conductive material 172 that connects to the inlay or using a transparent/semi-transparent conductive spray 179 as part of the lamination of the card that then touches electrical “posts” or conductive areas that are exposed during the manufacturing process (exposed copper or equivalent material that connects to the inlay much like
smart cards such as contact EMV). The material is then wired to the circuit and battery 180. As with exposed copper, a circuit is completed when both sides of the card are touched with a conductive material, such as fingers or for the purposes of this prototype, pliers 181. Conductive translucent coatings are available for use on the typical card PVC material. This method reduces power consumption of powered cards, while simplifying the user experience and reducing the chance of a powered card turning on accidentally within a pocket or wallet.

When power is first applied to the circuit, the switched output is not active. When the user completes the circuit by pinching in the conductive regions on both sides of the card, the output becomes active and is latched. If nothing touches the conductive regions on both sides of the card, the circuit will continue to output power until a timer is completed by the microprocessor, or unless both of the conductive planes are shorted again (e.g. the user pinches the powered card on conductive regions on both sides of the card). Upon initial power-up of the microprocessor, the microprocessor control pin is set to an input state. This allows for detection of additional touches of the conductive planes. When the card has finished its task, or a timeout condition occurs, the microprocessor can set the microprocessor control pin to an output, and an active low state will reset the latching circuit to a powered down state.

One embodiment of this latching circuit involves using an N-channel enhancement mode vertical DMOS FET. The enhancement mode feature means that if the gate voltage is zero (no touching) then the FET switch is OFF. When a person picks up a pinch power enabled card, he/she will naturally touch both sides of the card where the conductive material is around the edges of the card. Thus, the skin of the person closes the gate (short of this FET), thereby applying a voltage to the gate to turn on the FET. Once turned on, a timer on a microprocessor (or equivalent) can be programmed to turn off the powered card based on a set interval (a user programmable interval in one embodiment). When the gate reaches the battery voltage, the current flow will cease.

This "pinch power" approach solves two key problems with powered cards:

How to turn them on and off without cumbersome switches.

How to keep them from turning on when placed in areas that could activate a "switch" mechanism, such as a wallet, and thus needlessly drain the battery.

Dual Device Authentication: The second device 190 must authenticate with the private electronic vault (first device 189) before any information is passed or transaction performed. As shown in FIG. 17, two devices are dynamically paired when a random number 185 output from a high-quality random number generator 184 from within one device is input to the crypto chip 153 of the second device, and a SHA256 hash is generated by a key generator 183 between the random number 185 and some combination of the various identifiers 186. The generated pseudorandom number response 190 is then sent back to the first device, where it is compared by an internal comparator 182 with a SHA256 hash 193 of the same pseudorandom number generated 192 as that was challenged 185 and the same internal identifiers 191, all within the crypto chip 153 onboard the first device. If the two numbers match, the devices are authenticated.

Likewise, a one-time-use encryption key may be generated between devices in the same manner as authentication, in order to encrypt and store credit card numbers, names, and other private information on the private electronic vault. The temporary key may be stored in a temporary memory slot 188 within the crypto chip 153. The vault then sends encrypted data to the second device via a wireless communication link, where the encrypted data is decrypted via its internal one-time-use encryption key and then sent by the second device via the appropriate transaction method. For instance, if the transaction method is a common point of sale (POS) that utilizes magnetic stripe techniques, the second device may be a powered card with a reprogrammable dynamic magnetic stripe 163. Thus, the second device acts as a conduit to support virtually any method of payment or communications.

Dynamic codes are generated from combination of one or more unique identifiers and/or keys 187 that are specific to factors including but not limited to users, manufacturers, devices, accounts, locations and/or sessions or transactions. Identifiers that may be used within the dynamic pairing method include biometrics, proximity sensors, user "secrets" (Passwords/PINS/etc.), manufacturer ID, wallet ID, master encryption key, user customizable card names, card type, device serial number, electrical noise ID, CRC, MAC address, CVV, charge limits and time duration. A high-quality random number generator 184, Identifiers 187, embedded key generator 183, and comparator 182 are all safely hidden within the tamper-proof crypto chip 153 at all times. Even the proprietary dynamic pairing code algorithm used to generate the dynamic pairing codes may be stored in a tamper-proof crypto chip 153 as well, so that no information is ever available to be hacked.

The algorithm that generates the dynamic pairing code uses different combinations of these identifiers during different data sequences or different time instances in combination with a high quality random number generator 184 local on the same protected crypto chip 153 so that identifiers 187 saved on the device are never externally accessible. The combination of which identifiers are used and when they are used is based upon a proprietary NXT-ID (assignee of the present invention) algorithm. Thus, only the generated random number and its response are ever shared between the first and second devices.

Any second device, such as the dynamic card or even a cell phone, may be authenticated via dynamic pairing or equivalent method that sends a high quality random number 185 as a challenge to the other device, and compares the response 190 with its internally generated result. For second devices that are commercially available, such as cell phones, authentication codes may be generated by a SHA256 generator within software, or for more security for cell phone and other remote applications, the app can be in the middle of the 2 devices, where the app communicates from one device through the app to another device to ensure security at all times, even in demanding remote applications.

Challenge/response methods of authentication such as dynamic pairing have a distinct advantage of performing multi-factor authentication by passing only pseudorandom numbers, without revealing any identifiers or keys. Furthermore, having the pseudorandom number generator, comparator and the key generator within the same tamperproof device that also holds the identifiers ensures all secrets are kept secure during authentication and encryption key generation.

User Authentication: Users may access the private electronic vault by responding correctly to the authentication question from the vault. Questions could be preconfigured by the user or random. A user may be asked to speak a certain
word via a microphone 162, or provide a pattern 194 as shown in FIG. 18, password or pattern 195 as shown in FIG. 19.

Voice is a unique biometric in that a user may speak a typed word and a VoiceMatch™ algorithm that will recognize both the speaker and the word. In some embodiments, the user may simply give a spoken word correlated with specific private information, like a payment account or medical record. The private electronic vault will perform multi-factor authentication on this word by recognizing the speaker and the word itself. The word is then recognized as associated with the private information, and that information can then be sent to the second device. Additional security protection may be put in place, as a user desires, to require another authentication to display private data on the device.

Interfaces: The standard communication interface to the devices is BTLE (or for second devices, just simple Bluetooth), but the devices can also support other optional interfaces such as USB, or wireless interfaces such as NFC, RFID, infrared, optical acoustic, or WiFi. In some embodiments, these interfaces may be used by applications on the authenticated second device to communicate and control the private electronic wallet to add, delete, modify, manage and receive private information for some transaction. Private information that can be downloaded to the private electronic wallet may consist of payment, loyalty, identity, health, medical, or just about any information found within a typical wallet. Non-private information such as advertisements, coupons, shopping lists and the like may also be transferred to the private electronic wallet. In other embodiments, information may be scanned directly into the private electronic vault from a Square reader (a well known magnetic strip reader for mobile platforms), USB or Bluetooth standard magnetic strip reader for added security.

One advantage to this architecture of the private electronic vault is its standalone feature where all interfaces are controlled via end-to-end authentication and encryption so that no hacking can be achieved even when connected to other, more vulnerable devices such as cell phones and PCs (i.e., the second device of the system of the invention).

Validation process to enter data into wallet

One embodiment of the invention supports two validations processes

1. Name variation embedded in the private electronic vault
2. Validation process of payment cards prior to scanning.

When a user signs up for first time, she/he enters a last name and up to three variables for first, middle and nicknames. These names are then configured into specific write-only areas within the crypto chip of the electronic vault. As users load data from magnetic stripe cards, the private electronic vault parses the names swiped by a magnetic stripe reader and matches those names internal to its memory vault. If the names match, the card information is accepted and encrypted using a self generated encryption key that is also saved into internal secure memory. If additional names are needed, users may contact NXT-ID to allow more than three variations in an authorized name.

To further avoid card cloning, a user may submit all money-related cards to an approval process upon initial use, where the identity of the individual and the card are validated, and the bio key in a personal vault remotely. Once approved, the authentication key prevents other users from using the private electronic vault to program any new secondary devices. Only private information, such as payment accounts, approved by the approval process can be used by the electronic vault and dynamic card. Note, library, club membership cards and the like need not be approved if not desired by the user. Anyone trying to make a card from another individual’s private electronic vault would have to follow the same authentication process and therefore would be caught. When authentication is attempted between the devices and the user and the authentication key does not match, authorities can be notified to pursue the attempted clone. Combining this with other methods such as timeouts and/or number or type of products to be purchased further reduces theft and fraud.

Private Information Selection: Once private information is scanned or entered via the validation process, users may correlate the data to user-selected word(s) that act as aliases for the protected private information. These word(s) may be spoken and/or typed for security purposes. Alternatively, a user may also enter other biometrics and/or secrets as options to the private identity and payment vault to add further security to the user authentication process.

For instance, a user may wish to correlate “green gas card #3” to represent his or her Chase Visa credit card that he or she uses for payments for gasoline. When a user then wants this payment account, he or she would simply press the on button to activate the private electronic wallet and speak the previously recorded word representing the user’s associated private information (in this instance, his or her payment account associated with his or her Chase Visa credit card).

The word that the user speaks is then analyzed and compared to the previous word using a voice recognition algorithm internal to the private electronic vault. This algorithm identifies both the speaker and the word, and then programs the second (or payment) device with the Chase Visa credit card information and/or displays the information to a display on the local device as previously configured by the user.

Alternatively, a user may slide through each of the aliased word(s) 198 via a touch display and select the alias 198 that the user wishes to send to the second device. FIG. 20 describes the user interface (UI) 196 for the private electronic vault where users may select from user-configured aliases 198 that associate to some personal information within some user-configured categories 197 that has been stored to the vault. This user interface enables users to slide through a number of aliases 198 using a sliding gesture and/or buttons. The number of aliases (associated to captured personal information) is only limited by the memory configured on the device (defaults to 100 cards, but can support higher numbers with a larger memory chip).

As described in FIG. 21, the user interface (UI) may scroll through user-definable categories 200 on the private electronic vault where users may select a category of aliases 199. This menu is activated by pressing the “menu” button 199 (whose icon is obvious to those that have used current cell phone app technology), or by sliding left or right to open or close the menu.

This app may also be applied to other second devices that are authenticated. For instance, in the case of supporting a payment with a point of sale (PoS) system supporting magnetic stripe, a user may select the alias 198 by sliding through categories 199, selecting the appropriate category 200 the word(s) associated with the alias 198, or sliding through all categories 200 and aliases 198 on the vault; the vault then programs an authenticated second device, which in
turn programs its internal programmable magnetic stripe. In another embodiment, the alias could be selected by speaking into an application on an authenticated second device such as a cell phone, which then in turn commands the private electronic vault to select the appropriate alias and programs the authenticated second device with the programmable magnetic stripe.

[0091] Another user interface (UI) concept for a user to access categories 201 of aliases to personal information is shown in FIG. 22, while FIG. 23 describes another concept for a user to access preferred 202 aliases. FIGS. 24 and 25 illustrate a user interface (UI) concept for a user to view details 203 and 204 of private information such as a payment card.

[0092] As shown in FIG. 26, personal information and cards securely hidden within a private electronic vault may be managed from an app on a authenticated second device, such as mobile and fixed devices like cell phones, tablets, laptops, PCs and the like. Under this user interface (UI) personal information, such as payment cards, may be represented by logos, card pics, or other art 205 that a user may select from a browser 206. Settings 207 for each card may include alias names, transaction limits, etc. Once a card is scanned or entered into the private electronic vault, it appears as its correlated alias 208 (whatever alias name, logo, and settings given that personal information by the user). Categories 209 may also be programmed and loaded onto the private electronic vault from an authenticated app on a second device. From this management UI, a user may search various categories such as cards, coupons, receipts, etc.

[0093] Thus, according to one embodiment of this invention, private information is totally under the owner's control on the private electronic vault. The user may choose to display the private information on the private electronic vault itself, or send the private information from the vault itself using supported payment and/or communication methods optionally installed on the vault such as BTLE, NFC, dynamic magnetic stripe, EMV, QR and bar codes, infrared, acoustic, or WiFi. In other embodiments, the user has the added flexibility to interface to other authenticated second devices that then act as a conduit for the private information to be used to interface with other payment or communication methods. Once a transaction is completed, private information on the second device is zeroized by iteratively writing random ones and zeros over memory to make the second device "dumb" again and ensure all private information is destroyed. In this way, all private information is preserved 100% of the time as the second devices act as controls and/or conduits for the private information to support various communication and payment methods.

[0094] Security: One advantage of the approach of the various presented embodiments is security. Users can program the devices with any combination of the following security features:

[0095] User to Vault: Regardless if an authenticated second device is used or not, all users must be authenticated to the private electronic vault (the first device) using one of the following methods:

[0096] a. Biometrics 163 of FIG. 12: A biometric, such as voice, entered by the user matches that entered during setup (Note: Biometrics can include voice, gesture, finger, face, 3D face, IRIS, eye, eye vein, eye tracking, DNA, vein, palm, heartbeat, sweat, vibrometry, and/or scent by simply adding those sensors to the interface of the microprocessor).

[0097] b. PIN or Password: A PIN or password entered by the user matches that entered during setup.


[0099] d. Signature: The signature entered by the user matches that which was written on the rear and/or display of the device(s).

[1000] Private Data to Vault (i.e., the first device): Name variation embedded on the private electronic vault must match that scanned by any private information being input from certain types of cards such as payment, medical, and identity cards.

[0101] Card to a Card Company: The card is approved as valid by a financial or other institution providing the card.

[0102] Two paired devices: The two paired devices must be stolen under certain embodiments, not just the wallet.

[0103] a. Pairing: The second device(s) are dynamically paired to a specific private electronic vault.

[0104] b. Proximity: The second device(s) close proximity with a paired private electronic vault.

[0105] c. Name etching: A name may be permanently etched onto the private electronic vault (also referred to as the first device) to match other forms of identification of the user.

[0106] d. CVV, Names, Numbers and/or Expiration Dates: CVV, names, numbers and/or expiration dates may be displayed on the device(s).

[0107] e. Charge limits: The transaction does not exceed the amount limit set by the owner of the private information.

[0108] f. Time duration: The time duration for a transaction or account does not exceed the set by the owner of the private information.

[0109] h. Dynamic Authentication and Encryption keys: One-time use authentication and encryption keys that are generated dynamically based on the time of day and/or sequence, and/or a combination of the identifiers.

[0110] In some embodiments, the private electronic vault (i.e., the first device) and the second device must both be present for any transaction to take place. Pairing the device(s) reduces theft and fraud by requiring both devices to be present and authenticated with one another prior to any transaction that accesses private information. This significantly limits the ability of thieves to clone cards, for instance, since both devices must be present to program the first device (electronic vault), and they are further protected with a key derived from the combination of methods described.

[0111] The user may additionally set further limitations before the transaction takes place. Users can select any or a combination of methods including biometrics, proximity sensors, time out periods, maximum dollar amount, number of transactions, type of transactions, or user selected products that are allowed to be purchased. If these limitations are exceeded, the devices immediately detect the anomaly and theft or fraud can be prevented, and authorities can be notified.

[0112] Limitations at the point of sale reduce the impact of fraud while keeping within the bounds of current transaction and payment technologies. These methods of security are advantageous to "end-to-end" solutions, since they apply...
limitations to access private information prior to any transaction and under full control by the user. Enabling the user to set limitations for use of the device(s) is also advantageous, since it occurs prior to any release of private information or point of sale, and the variability of settings will act as a further deterrent to thieves and fraud abusers. In addition, under this invention, the merchant need not be involved at all. Security is maintained without impact to the merchant in any way.

The methods of the present invention can also be extended to other mobile devices acting as the private electronic wallet. These methods may also be extended such that a mobile device authenticates directly to a second device, such as a dynamic magnetic stripe card. However, a severed configuration is advantageous, given it significantly reduces the vulnerabilities that still plague the mobile wireless device industry by providing a standalone, separate device that is virtually hack proof.

Integration with 3rd Party Mobile Applications: The private electronic wallet can be used standalone or tethered to mobile or fixed devices such as a cell phone or PC and driven by third party apps and user interfaces on those devices. Security is maintained at all times by use of dynamic pairing or equivalent authentication and encryption between the private electronic vault and any of these second devices such as PCs, mobile devices and/or programmable dynamic stripe cards. Basic configurations of the private electronic vault support BTLE to configure and validate the user. Other configurations include USB and wireless configurations such as NFC, RFID, WiFi, 3G/4G/LTE and Bluetooth, although each of these configurations has separate wireless security profiles.

Differences with other implementations of a digital wallet: The unique features of the present invention and its described first and second devices that separate the invention from all other prior art implementations include:

A separate solution dedicated to the purpose of an electronic wallet, versus cell phones and other mobile devices that are multi-purpose.

Two separate devices that must be “dynamically paired” to each other.

Sufficiently small to support a number of different configurations, including:

Part of the physical wallet or standalone wallet insert

Money clip

Key chain accessory

Watch

Dongle

Cell Phone accessory

or any other device typically carried by an individual.

Support the most common forms of payment today:

Magnetic Stripe

NFC

EMV

QR Codes

RFID

In other embodiments, infrared, acoustic, Bluetooth Low Energy (BTLE), WiFi, 3G/4G/LTE and cloud based payment forms are also supported.

Replication of all cards and other information frequently found within a typical physical wallet, not just payment cards, including:

Payment cards

Credit

Debit

ATM

Gift

Cash

Calling

Loyalty cards

Shopping (Restaurants, Retail, etc.)

Frequent Flyer

Reward Cards

Club/Membership cards

Shopping (BJ’s, Sam’s Club, etc.)

Organizations/Affiliations (IEEE, etc.)

Social

Library

Hotel

Rental Car

Vacation

Roadside assistance

Identity

Licenses

Passports

Visas

Voter’s Registration

Employee

Security

Passcards

Business Cards

Insurance

Auto

Health/Medical

Dental

House

Life

Travel

Medical Records Cards

Conditions

Medications

Hospitalization

Shopping lists

Discount

Coupons

Receipts

Tickets

Enhanced Security features including:

User to Vault

Private Information to Vault

Card to Card Company

Two Separate Dynamically Paired devices as described herein

Pairing of external devices to the first device (the private electronic wallet)

Proximity

PIN or Password

Pattern

Signature

Name etching

CVV

Biometric enabled generated keys

Charge limits

Time duration
Dynamic authentication and encryption keys (based on dynamic combinations of information listed above).

Other Services: Unique services that may be integrated with this private electronic wallet technology include:

Receipts (Pocket Accountant)
Automatic Receipt Coding and Book Keeping
Shopping List
Shopping Assistant (Shopper and/or Retail Aisle Assistant)

Ads/Specials/Coupons
Proximity Based Ads/Specials/Coupons
RFID Ads/Specials/Coupons
Proximity Cards
Toll Attendant
Money (Wires)
Payment
24 hour Replacement Service
Travel Service.

The following describes each of these services:

Receipts (Pocket Accountant): For transactions that utilize 2-way communications with servers, such as wireless/contactless methods such as NFC, RFID, WiFi and 3G/4G/LTE, transactions can be recorded directly to the first device (private electronic wallet) so that it acts as a “pocket accountant”. Within this embodiment of this invention, information regarding the card such as balances can also be displayed with each soft-card.

Automatic Receipt Coding and Book Keeping: For transactions that utilize 2-way communications with servers, such as wireless/contactless methods such as NFC, RFID, WiFi and 3G/4G/LTE, transactions can be automatically recorded, coded, sorted and output to third party programs such as excel and QuickBooks. Within this embodiment of this invention, information regarding the transactions of a card can be automatically output to business accounting tools.

Shopping List: Products can be typed, scanned or electronically obtained on a PC or mobile device, and downloaded to the Wocket™ to be used at a retail location.

Shopping Assistant (Wocket™ Shopper and/or Retail Aisle Assistant): This invention detects RFID enabled products as a shopper strolls down a retail aisle and notifies the shopper of any product that matches an item on a shopping list previously downloaded to the private electronic wallet or vault, commercially referred to as the Wocket™

Ads/Specials/Coupons: This invention consists of advertisements, specials and coupons that can be automatically offered to the shopper (user) based upon the store the user enters. The store location is detected by the private electronic vault via optional integrated GPS module, or via wireless integration with a user’s cell phone.

RFID Ads/Specials/Coupons: This embodiment consists of advertisements, specials and coupons that can be automatically sent to the vault from the retail item itself as a shopper passes within range of the RFID of the specific retail item (or product). The shopper can then be notified of “specials” (coupons) that can be used with the product.

Proximity Cards: Cards can be automatically offered to the shopper (user) based upon the store the user enters. In this embodiment the store location is detected by the vault via optional integrated GPS module, or via wireless integration with a user’s cell phone. The best cards are offered to the shopper based on calculating which card provides the best benefits for a given store or list of purchases.

Toll Attendant: The private electronic vault is also integrated with novel RFID that can be used as a passive mobile “Toll” payment method. The toll attendant service automatically interfaces with the same RFID technology of the E-ZPass Interagency Group (IAG), which comprises 25 agencies spread across 14 states.

Money (Wires): This service enables the private electronic wallet to transfer money to one another via a wallet to wallet validation process. Once validated, payments can take place between two parties with proper authentication of each of their respective Wockets.

Payment: The embodiment of this invention enables a private electronic wallet to accept payments. Consumers can pay for items via their typical payment method including magnetic stripe, NFC, contactless EMV, and QR Codes. The private electronic wallet can be configured to accept these forms of payment with connected or disconnected methods of validation (wireless payment validation and/or pre-authorization via housing each of the cards prior to transaction (so that they can be held securely until the validation process can be performed)).

24 hour Replacement Service: This embodiment provides an optional service to users to replace the private electronic wallet by calling the service number, validating the user’s identity, and sending a new Wocket with all cards that have been placed by the user on the secure server.

Travel Service: This embodiment comprises an optional service that enables users to notify card companies of cards on a specific private electronic wallet of impending travel plans, to prevent the card company from calling the user to validate purchases as the user travels.

What is claimed is:
1. A method for storing and using personal information, comprising:
   storing the personal information on a first device;
   authenticating the first device to a second device; and
   transferring the personal information from the first to the second device.
2. The method of claim 1 further comprising the second device conducting a transaction related to the personal information.
3. The method of claim 2 wherein the personal information comprises information associated with a payment card, the second device replicating the information associated with the payment card and the transaction comprises paying for an item or service using the second device.

4. The method of claim 1 wherein the transaction involves one or more of financial information, medical information and identity information.

5. The method of claim 1 further comprising authenticating a user to the first and second devices prior to transferring the personal information from the first device to the second device.

6. The method of claim 1 wherein the personal information is associated with a user-configured alias comprising at least one of a written or spoken word stored within a memory of the first device, the first device recognizing the alias and selecting the associated personal information.

7. The method of claim 6 wherein the alias comprises one or more keywords for configuring the second device according to a desired payment transaction method.

8. The method of claim 1 further comprising erasing an item of the personal information by randomly writing 1’s and 0’s over the personal information.

9. The method of claim 8 wherein the step of erasing is executed after the item of personal information has been accessed a predetermined number of times or after a predetermined time interval from storing the item of personal information on the first device.

10. The method of claim 1 further comprising at least one of the first device and the second device entering a sleep state after a period of inactivity.

11. The method of claim 10 further comprising awakening the first device by operation of a third device communicating with at least one of the first and second devices.

12. The method of claim 1 wherein the second device comprises a dynamically programmable magnet stripe.

13. The method of claim 1 wherein the step of transferring is executed over an encrypted communications link.

14. The method of claim 1 further comprising the second device using the personal information to perform a transaction or an action.

15. The method of claim 1 wherein a third device controls operation of at least one of the first and the second devices.

16. The method of claim 15 wherein the third device comprises one or more of a cell phone, a personal computer, a laptop computer, a notebook computer, and a device controlled by a microprocessor or microcomputer.

17. A system for storing and using personal information, comprising:
   a first device for storing the personal information;
   a second device authenticated to the first device, the personal information transferred from the first device to the second device after authentication between the first and the second devices, the second device using the personal information in a transaction or action by replicating the personal information in a format according to a desired transaction or action.

18. The system of claim 17 wherein a third device controls operation of at least one of the first and the second devices.

19. The system of claim 17 wherein the second device comprises a dynamically programmable magnet stripe.

20. The system of claim 17 wherein the personal information comprises one or more of financial information, medical information and identity information.