US 20090255996A1

(19) **United States**

(12) **Patent Application Publication**

Brown et al.

(10) **Pub. No.: US 2009/0255996 A1**

(43) **Pub. Date: Oct. 15, 2009**

(54) **THREE-LEGACY MODE PAYMENT CARD WITH PARAMETRIC AUTHENTICATION AND DATA INPUT ELEMENTS**

(76) Inventors: **Kerry D. Brown**, Portola Valley, CA (US); **Daniel Chatelain**, Emerald Hills, CA (US)

Correspondence Address:
Richard Brewster Main, Esq.
Patents Pending, 9832 Lois Stiltner Court
Elk Grove, CA 95624 (US)

(21) Appl. No.: **12/489,662**

(22) Filed: **Jun. 23, 2009**

Related U.S. Application Data

(60) Division of application No. 10/800,821, filed on Mar. 15, 2004, Continuation-in-part of application No. 10/738,376, filed on Dec. 17, 2003, now Pat. No. 7,044,394.

Publication Classification

(51) **Int. Cl.**
G06K 19/06 (2006.01)

(52) **U.S. Cl.** **235/493**

(57) **ABSTRACT**

A payment card comprises a plastic card and operates with three different legacy payment systems. A magnetic stripe with user account data allows card use in traditional point-of-sale magnetic card readers. A dual-input crypto-processor embedded in the card provides for contact/contactless smart card operation. A user input provides for user authentication by the crypto-processor. Internal to the plastic card, and behind the magnetic stripe, a magnetic array includes a number of fixed-position magnetic write heads that allow the user account data to be automatically modified by the crypto-processor.

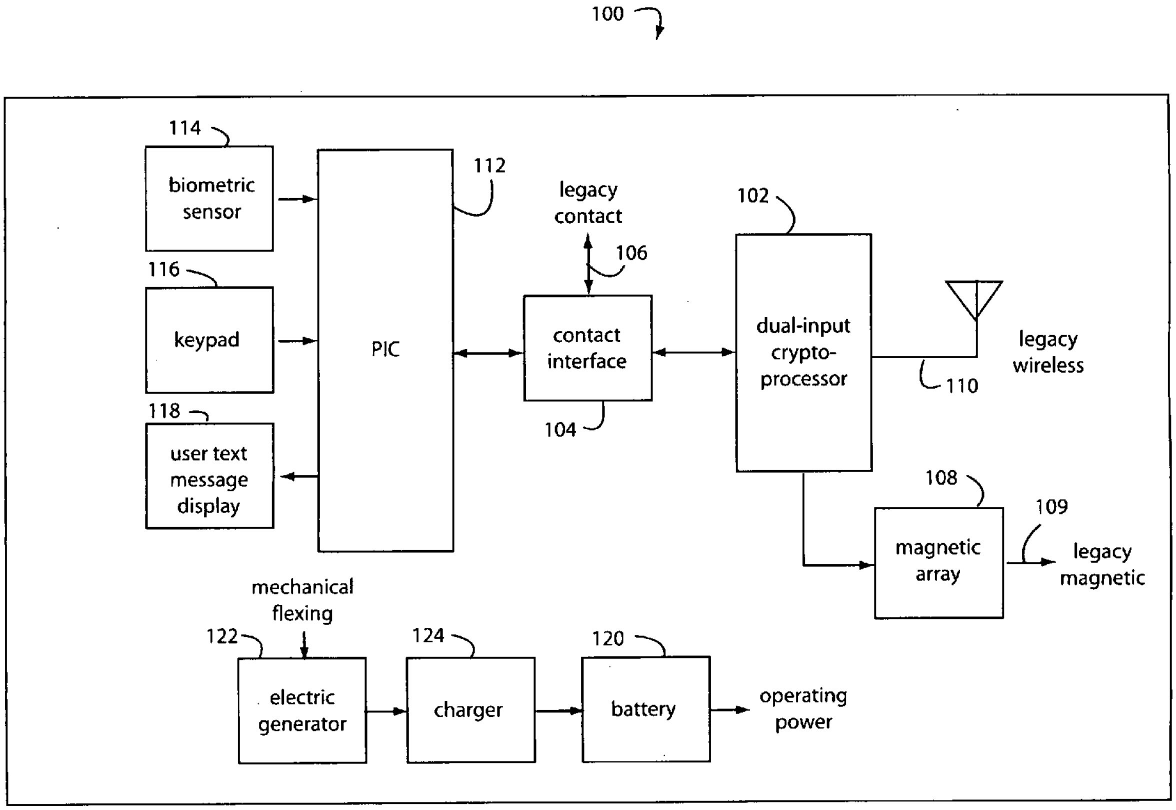


Fig. 1

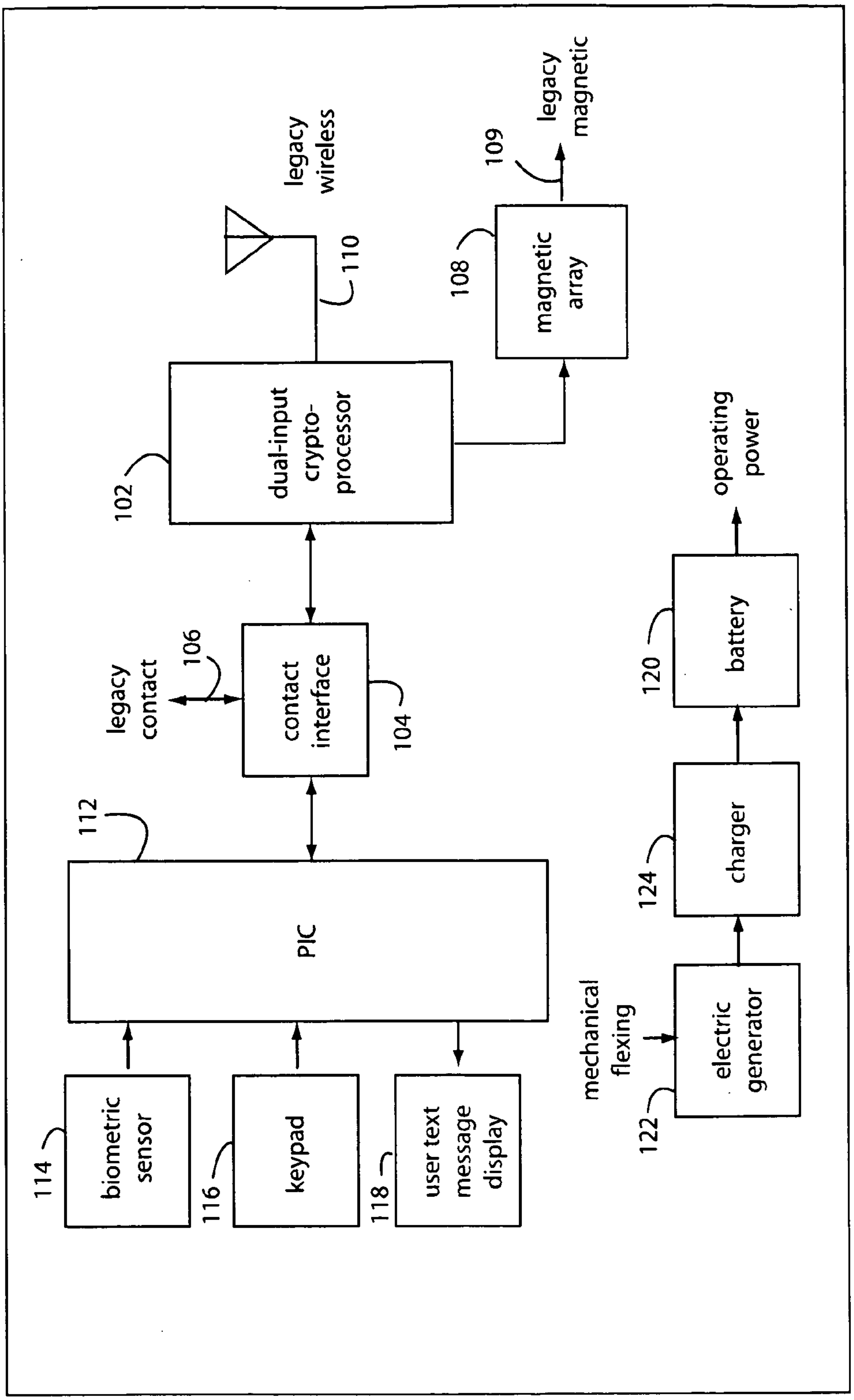
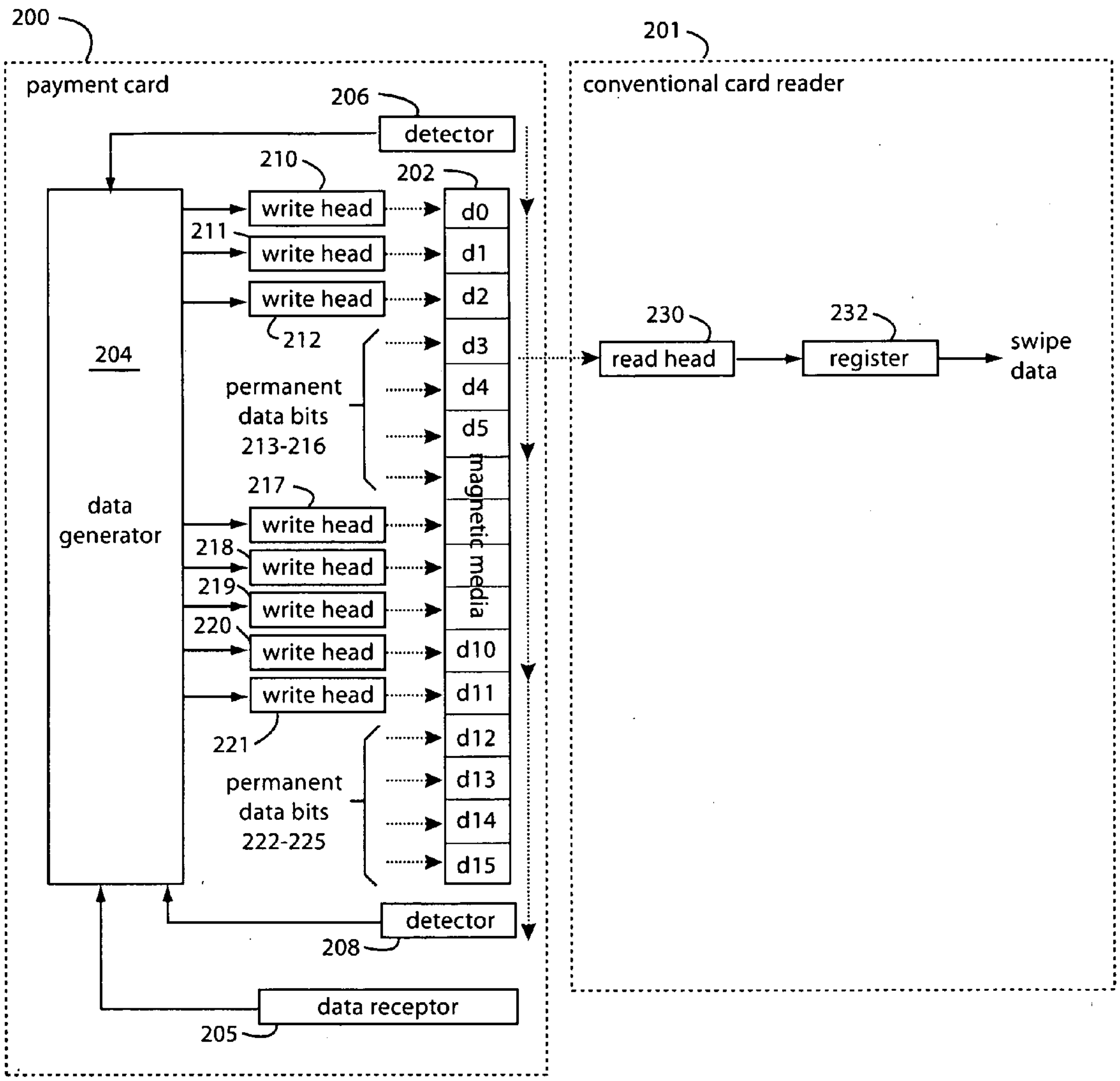

100
biometric sensor
114
keypad
116
user text message display
118
PIC
112
contact interface
104
legacy contact
106
dual-input crypto-processor
102
legacy wireless
110
magnetic array
108
legacy magnetic
109
mechanical flexing
electric generator
122
charger
124
battery
120
operating power

Fig. 2


200
payment card
206
detector
210
202
write head
d0
211
write head
d1
write head
d2
212
204
data generator
d3
permanent data bits 213-216
d4
d5
magnetic media
217
write head
218
write head
219
write head
220
write head
d10
write head
d11
221
d12
permanent data bits 222-225
d13
d14
d15
detector
208
data receptor
205
201
conventional card reader
230
read head
232
register
swipe data

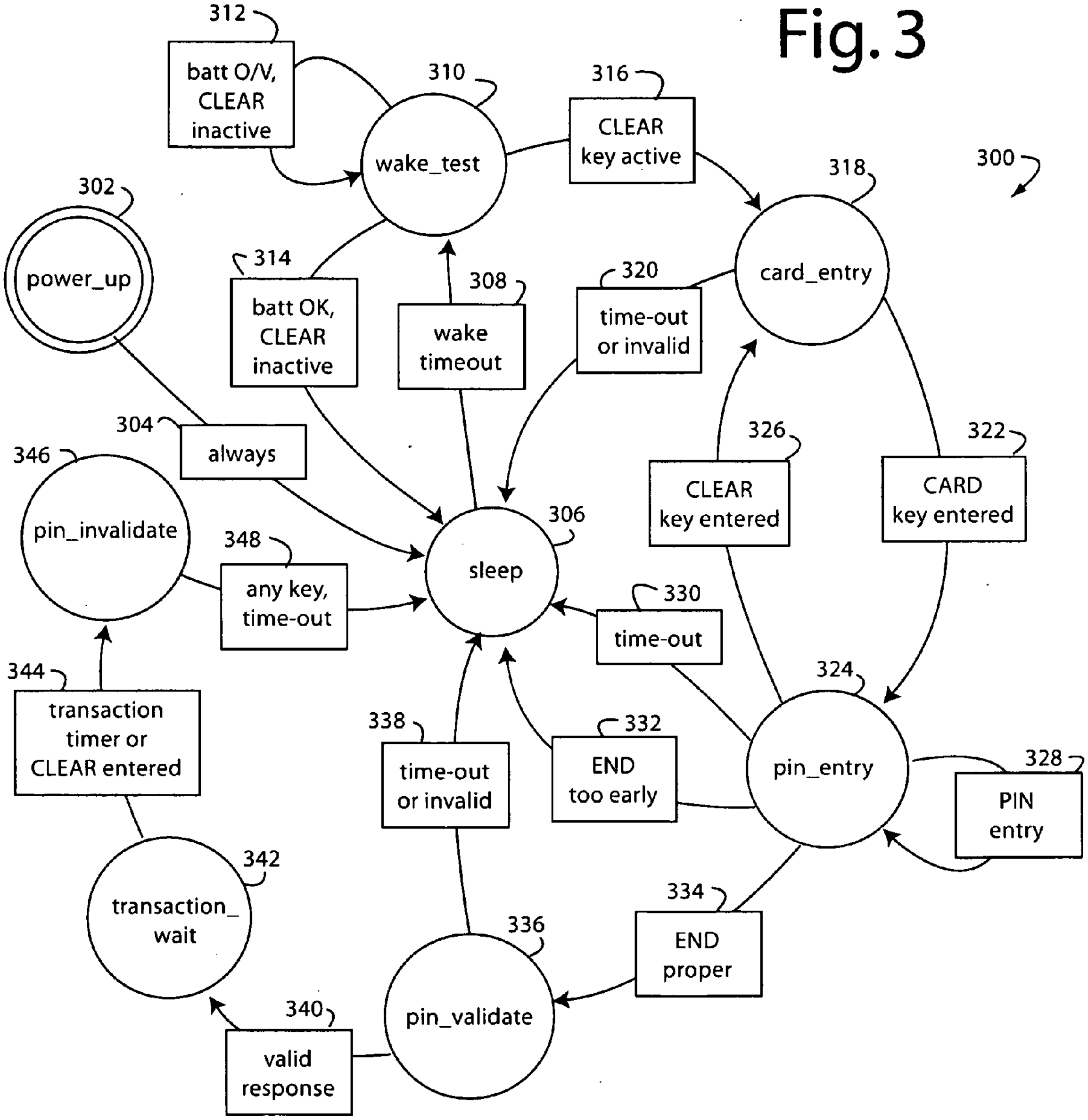


Fig. 3
300
302
power_up
304
always
306
sleep
308
wake timeout
310
wake_test
312
batt O/V, CLEAR inactive
314
batt OK, CLEAR inactive
316
CLEAR key active
318
card_entry
320
time-out or invalid
322
CARD key entered
324
pin_entry
326
CLEAR key entered
328
PIN entry
330
time-out
332
END too early
334
END proper
336
pin_validate
338
time-out or invalid
340
valid response
342
transaction_ wait
344
transaction timer or CLEAR entered
346
pin_invalidate
348
any key, time-out

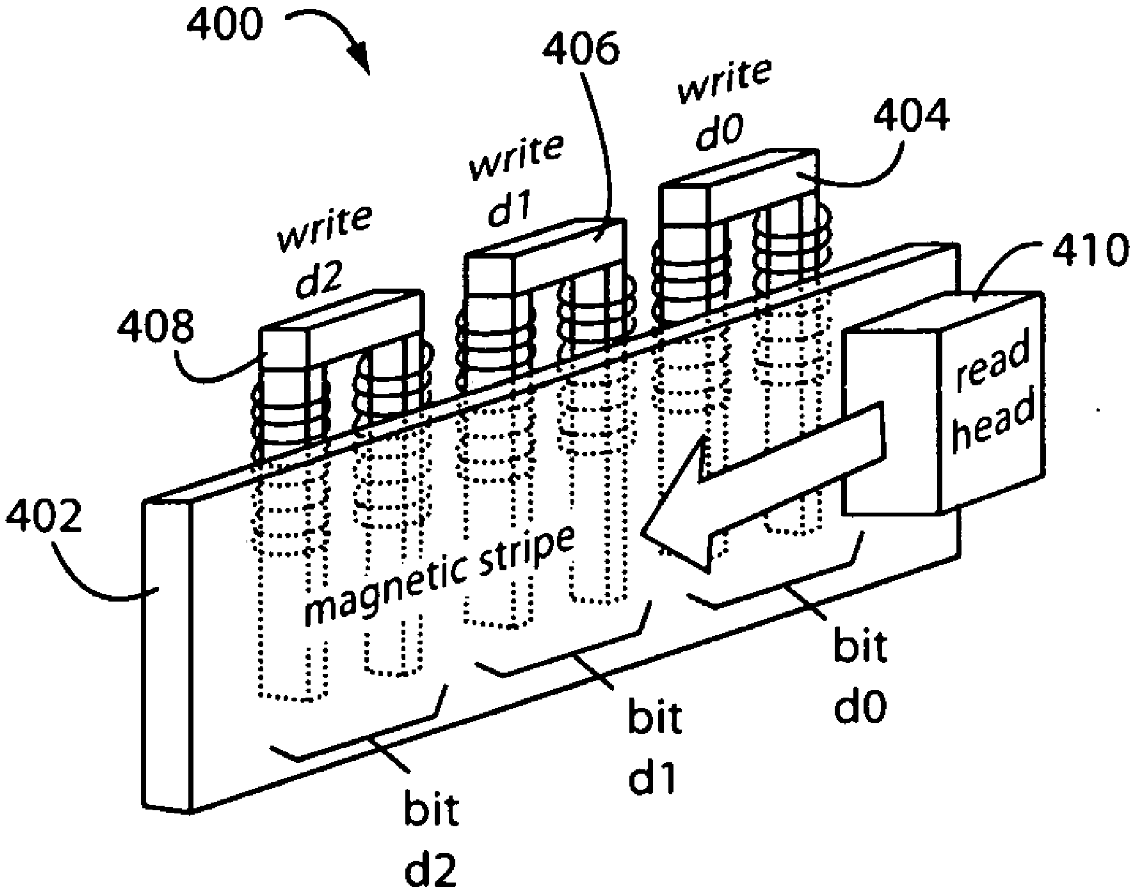

400
406
write d0
write d1
write d2
404
410
408
read head
402
magnetic stripe
bit d0
bit d1
bit d2

Fig. 4

THREE-LEGACY MODE PAYMENT CARD WITH PARAMETRIC AUTHENTICATION AND DATA INPUT ELEMENTS

RELATED APPLICATION

[0001] This Application is a Divisional of U.S. patent application Ser. No. 10/800,821, filed Mar. 15, 2004, by the present inventor, Kerry D. BROWN, and titled PAYMENT CARD WITH PARTIAL DYNAMIC MAGNETIC ACCOUNT DATA AND TIMEOUT. Such was, in turn, a Continuation-In-Part of an Application that is now U.S. Pat. No. 7,044,394, issued May 16, 2006, titled PROGRAMMABLE MAGNETIC DATA STORAGE CARD. These are incorporated by reference as if fully set forth herein.

BACKGROUND OF THE INVENTION

[0002] 1. Field of the Invention

[0003] The present invention relates to a payment card, and more particularly to payment cards with contact/contactless smartcard interfaces, and an internally writeable magnetic data stripe readable by legacy card readers.

[0004] 2. Description of Related Art

[0005] Credit card and debit card use and systems have become ubiquitous throughout the world. Originally, credit cards simply carried raised numbers that were transferred to a carbon copy with a card-swiping machine. The merchant simply accepted any card presented. Spending limits and printed lists of lost/stolen cards were ineffective in preventing fraud and other financial losses. So merchants were required to telephone a transaction authorization center to get pre-approval of the transaction. These pre-approvals were initially required only for purchases above a certain threshold, but as time went on the amounts needing authorization dropped lower and lower. The volume of telephone traffic grew too great, and more automated authorization systems allowed faster, easier, and verified transactions. Magnetic stripes on the backs of these payment cards started to appear and that allowed computers to be used at both ends of the call.

[0006] The magnetic data on the stripe on the back of payment cards now contains a standardized format and encoding. The raised letters and numbers on the plastic cards are now rarely used or even read. This then gave rise to "skimming" devices that could be used by some unscrupulous merchant employees to electronically scan and save the information from many customers' cards. Reproducing an embossed card complete with photos is then rather easy.

[0007] Smartcards were first introduced around 1994 with embedded single-chip cryptoprocessors and contact interfaces. These required a new reader that could probe the smartcard's contact pad and electronically interrogate the card. Cards could be authenticated this way, but the contact interfaces proved to be troublesome. Such cards have not gained wide acceptance because new readers needed to be installed.

[0008] Dual interface smartcards started to appear around 2000. Such supported both contact (e.g., ISO/IEC-7816) and contactless (e.g., ISO/IEC-14443) interfaces, and used two completely independent cryptoprocessors and interfaces. They are therefore relatively expensive, because of the duplication. The independence of the two cryptoprocessors and interfaces meant that each had to be updated individually, the two may not talk to one another.

[0009] Typical dual interface smart cards support both contact and Type-A and/or Type-B antenna structures and the corresponding operating frequencies. Type A has a range of about 10 cm, and type B has a range of about 5 cm. Type B supports a higher data rate, but has proven to be the less popular because of the shorter range.

[0010] Dual-input smartcard cryptoprocessors started to become available in 2004, e.g., Philips Semiconductors family of 8-bit MIFARE® PROX dual interface smart card controllers. These use one IC with a crypto co-processor that has both contact and contactless interfaces. Updating the data through either interface is effective for both interfaces. The total cost of a smartcard using dual-input devices is much closer to the original single-chip cryptoprocessors with contact interfaces.

[0011] The proliferation of magnetic, contact, and contactless technologies is causing chaos, and the huge installed base of magnetic point-of-sale readers in the United States has been inhibiting the transition to smartcards, a USA cost, estimated by American Express in 2002, of approximately $4-14 billion dollars. What is needed is a transitional payment card that can continue to support magnetic reading while also being able to respond to smartcard readers. It further would be advantageous to have a payment card that can self-authenticate its users. Additionally, a card with EMV (Europay-MasterCard-Visa) security features of a smartcard and the transaction communications features compatible with magnetic stripe transaction acceptance systems and processing infrastructure.

SUMMARY OF THE INVENTION

[0012] Briefly, a payment card embodiment of the present invention comprises electronic components disposed in a plastic card base needed to operate with magnetic reader, contact, and contactless legacy card payment systems. A magnetic stripe with user account data allows card use in traditional point-of-sale magnetic card readers. A dual-input crypto-processor embedded in the card provides for contact/contactless smart card operation. A user input provides for user authentication by the crypto-processor. Internal to the plastic card, and behind the magnetic stripe, a magnetic array includes a number of fixed-position magnetic write heads that allow the user account data to be automatically modified by the crypto-processor and support circuitry.

[0013] The above and still further objects, features, and advantages of the present invention will become apparent upon consideration of the following detailed description of specific embodiments thereof, especially when taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] FIG. **1** is a functional block diagram of a payment card embodiment of the present invention;

[0015] FIG. **2** is a functional block diagram of a legacy magnetic card and reader embodiment of the present invention;

[0016] FIG. **3** is a state diagram of a card authentication process embodiment of the present invention; and

[0017] FIG. **4** is a perspective diagram of a magnetic array embodiment of the present invention as can be used in the devices of FIGS. **1**-**3**.

DETAILED DESCRIPTION OF THE INVENTION

[0018] FIG. **1** illustrates a payment card embodiment of the present invention, and is referred to herein by the general reference numeral **100**. Payment card **100** operates in any of three ways, e.g., (a) as a typical magnetic stripe card, (b) as a typical contact-mode smart card, and (c) as a typical wireless (proximity) smart card. It is implemented in the familiar credit/debit card format as a plastic wallet card with a magnetic stripe on its back. For example, in the ISO/IEC-7810 format. The payment card **100** comprises a dual-input crypto-processor **102** with a contact interface **104**, e.g., ISO/IEC-7816. For example, a Philips Semiconductor type P8RF6016 triple-DES secure dual interface smart card IC could be used. Surface contacts on the card provide a conventional legacy contact **106** that can be used by traditional contact-mode card readers. A magnetic array **108** is arranged on the back of the card and presents what appears to be an ordinary magnetic stripe **109** encoded with appropriate bank and user information for a conventional magnetic card reader. Such readers are ubiquitous throughout the world at point-of-sale terminals. An antenna **110** provides wireless interface to conventional wireless smart card readers, e.g., ISO/IEC-14443-2 which operates at 13.56 MHz.

[0019] Particular details on the construction and operation of the magnetic array are included in a parent of the present application, U.S. Pat. No. 7,044,394, issued May 16, 2006, titled PROGRAMMABLE MAGNETIC DATA STORAGE CARD. Data sent to the magnetic array **108** can be withheld until the user authenticates themselves to the smartcard **100**. And such data will only be readable by a magnetic reader or smartcard reader for only a limited time or limited number of swipes or contact/contactless transactions.

[0020] An economic way of implementing payment card **100** is to use commercially available dual-input crypto-processors for processor **102** because they inherently come with the contact interface **104**. This then can be easily interfaced to a low-power microcontroller **112**, e.g., a Microchip programmable interface controller (PIC). In one embodiment, the payment card **100** includes a biometric sensor **114** that can sense some physical attribute about the user. For example, a fingerprint or signature input through a scanner or pressure sensor array. In other embodiments, the payment card **100** includes a keypad **116** with which a user can select a card personality and enter a personal identification number (PIN), password, or other data. Such personality selection can, e.g., be a choice amongst VISA, MasterCard, American Express, etc., so the payment card **100** presents the corresponding account and user numbers in the required formats for the particular bank and payment processor. A liquid crystal display (LCD) **118** in its simplest form presents a blinking indication that keypad input has been accepted, the card is awake and active, etc. A more complex LCD **118** can be used to display text message to the user in alternative embodiments of the present invention.

[0021] The communication between PIC **112** and dual-input crypto-processor **102** is such that each digit of a PIN entered is forwarded as it is entered. The whole PIN is not sent essentially in parallel. Such strategy makes the hacking of the card and access to user data more difficult. The PIC **112** does not store the PIN, only individual digits and only long enough to receive them from the keypad **116** and forward them on.

[0022] An embedded power source is needed by payment card **100** that can last for the needed service life of a typical smartcard, e.g., about eighteen months to four years. A battery **120** is included. In more complex embodiments, a piezoelectric generator **122** and charger **124** can be used that converts incidental temperature excursions and mechanical flexing of the card into electrical power that can charge a storage capacitor or help maintain battery **120**. The piezoelectric generator **122** comprises a piezoelectric crystal arranged, e.g., to receive mechanical energy from card flexing and/or keypad use. The charger **124** converts the alternating current (AC) received into direct current (DC) and steps it up to a voltage that will charge the battery. Alternative embodiments can include embedded photovoltaic cells to power the card or charge the battery.

[0023] FIG. **2** illustrates a payment card embodiment of the present invention, and is referred to herein by the general reference numeral **200**. In particular, FIG. **2** details the way magnetic array **108** and the legacy magnetic interface **109** can operate in the context of FIG. **1**.

[0024] A conventional, "legacy", merchant point-of-sale magnetic-stripe card reader **201** is used to read user account data recorded on a magnetic stripe **202** on the payment card **200**. Such is used by a merchant in a traditional way, the payment card **200** appears and functions equivalent to an ordinary debit, credit, loyalty, prepay, and similar cards with a magnetic stripe on the back.

[0025] User account data is recorded on the magnetic stripe **202** using industry-standard formats and encoding. For example, ISO/IEC-7810, ISO/IEC-7811(-1:6), and ISO/IEC-7813, available from American National Standards Institute (NYC, N.Y.). These standards specify the physical characteristics of the cards, embossing, low-coercivity magnetic stripe media characteristics, location of embossed characters, location of data tracks 2-3, high-coercivity magnetic stripe media characteristics, and financial transaction cards. A typical Track-1, as defined by the International Air Transport Association (IATA), is seventy-nine alphanumeric characters recorded at 210-bits-per-inch (bpi) with 7-bit encoding. A typical Track-2, as defined by the American Bankers Association (ABA), is forty numeric characters at 75-bpi with 5-bit encoding, and Track-3 (ISO/IEC-4909) is typically one hundred and seven numeric characters at 210-bpi with 5-bit encoding. Each track has starting and ending sentinels, and a longitudinal redundancy check character (LRC). The Track-1 format includes user primary account information, user name, expiration date, service code, and discretionary data. These tracks conform to the ISO/IEC/IEC Standards 7810, 7811-1-6, and 7813, or other suitable formats.

[0026] The magnetic stripe **202** is located on the back surface of payment card **200**. A data generator **204**, e.g., implemented with a microprocessor, receives its initial programming and personalization data from a data receptor **205**. For example, such data receptor **205** can be implemented as a serial inductor placed under the magnetic stripe which is excited by a standard magnetic card writer. Additionally, the data may be installed at the card issuer, bank agency, or manufacturer by existing legacy methods. The data received is stored in non-volatile memory. Alternatively, the data receptor **205** can be a radio frequency antenna and receiver, typical to ISO/IEC/IEC Specifications 24443 and 25693. The data generator **204** may be part of a secure processor that can do cryptographic processing, similar to Europay-Mastercard-Visa (EMV) cryptoprocessors used in prior art "smart cards".

[0027] Card-swipes generate detection sensing signals from one or a pair of detectors **206** and **208**. These are embedded at one or each end of magnetic stripe **202** and can sense the typical pressure applied by a magnetic read head in a scanner. A first set of magnetic-transducer write heads **210-212** are located immediately under bit positions d**0**-d**2** of magnetic stripe **202**. The data values of these bits can be controlled by data generator **204**. Therefore, bit positions d**0**-d**2** are programmable.

[0028] Such set of magnetic-transducer write heads **210-212** constitutes an array that can be fabricated as a single device and applied in many other applications besides payment cards. Embodiments of the present invention combine parallel fixed-position write heads on one side of a thin, planar magnetic media, and a moving serial read head on the opposite side. Such operation resembles a parallel-in, serial-out shift register.

[0029] A next set of bit positions **213-216** (d**3**-d**6**) of magnetic stripe **202** are fixed, and not programmable by data generator **204**. A conventional card programmer is used by the card issuer to program these data bits. A second set of magnetic write heads **217-221** are located under bit positions d**7**-d**11** of magnetic stripe **202**. The data values of these bits can also be controlled by data generator **204** and are therefore programmable. A last set of bit positions **222-225** (d**12**-d**15**) of magnetic stripe **202** are fixed, and not programmable by data generator **204**. In alternative embodiments of the present invention, as few as one bit is programmable with a corresponding write head connected to data generator **204**, or as many as all of the bits in all of the tracks.

[0030] The legacy card reader **201** is a conventional commercial unit as are already typically deployed throughout the world, but especially in the United States. Such deployment in the United States is so deep and widespread, that conversion to contact and contactless smartcard systems has been inhibited by merchant reluctance for more purchases, employee training, counter space, and other concerns.

[0031] It is an important aspect of the present invention that the outward use of the payment card **200** not require any modification of the behavior of the user, nor require any special types of card readers **201**. Such is a distinguishing characteristic and a principle reason that embodiments of the present invention would be commercially successful. The card reader **201** has a magnetic-transducer read head **230** that is manually translated along the length of data stripe **202**. It serially reads data bits d**0**-d**15** and these are converted to parallel digital data by a register **232**.

[0032] The magnetic-transducer write heads **210-212** and **217-221** must be very thin and small, as they must fit within the relatively thin body of a plastic payment card, and be packed dense enough to conform to the standard recording bit densities. Integrated combinations of micro-electro-mechanical systems (MEMS) nanotechnology, and longitudinal and perpendicular ferromagnetics are therefore useful in implementations that use standard semiconductor and magnetic recording thin-film technologies.

[0033] FIG. **3** represents a card authentication process embodiment of the present invention, and is referred to herein by the general reference numeral **300**. Such process details the way that the processor **102** (FIG. **1**) interacts with keypad **116** and LCD **118** in one embodiment of the present invention. Here, the keypad includes digits 0-9, CLEAR, and ENTER keys.

[0034] Process **300** comprises a power_up state **302** that passes through an "always" condition **304** to a sleep state **306**. A "wake timeout" condition **308** occurs when a wake-up timer times out. A wake_test state **310** checks battery condition and the CLEAR key. A condition **312** causes a loop back if the battery is within proper operating voltage range and the CLEAR key is inactive. If the battery is in range and the CLEAR key is inactive, a condition **314** returns to sleep state **306**. But if the user has pressed the CLEAR key, a condition **316** passes to a card_entry state **318**. The LCD is caused to blink at 1.0 Hz. A time-out for waiting for another key to be pressed, or an invalid key being entered, causes a condition **320** to return to sleep process **306**.

[0035] If a CARD key is entered, a condition **322** passes to a pin_entry state **324**. If CLEAR key was entered, a condition **326** returns to card_entry state **318**. The LCD is caused to blink at 1.0 Hz. A PIN entry condition **328** processes each entry. If the user takes too long to enter the PIN, a time-out condition **330** returns to sleep state **306**. If the ENTER key is pressed too soon, e.g., not enough PIN digits have been entered, a condition **332** returns to sleep state **306**. If a proper number of PIN digit entries have been made, and that was followed by the ENTER key, a condition **334** passes to a pin_validate state **336**.

[0036] If the PIN entered is invalid or a time-out has occurred, a condition **338** returns to sleep state **306**. Otherwise, a valid-response condition **340** passes to a transaction_wait state **342**. The LCD is caused to blink at 0.5 Hz. A transaction timer or CLEAR key entered condition **344** passes to a pin_invalidate state **346**. Any key being pressed or a time-out in a condition **348** passes to the sleep state **306**. This process may be used in conjunction with a smart card cryptoprocessor to unlock encrypted card data to be released for legacy transaction processes described herein and typical for magnetic stripe and smart cards.

[0037] FIG. **4** illustrates a magnetic data storage array embodiment of the present invention, and is referred to by the general reference numeral **400**. The magnetic data storage array **400** includes a magnetic stripe **402** that mimics those commonly found on the backs of credit cards, debit cards, access cards, and drivers licenses. In alternative embodiments of the present invention, array **400** can be a two-dimensional array, and not just a single track.

[0038] Here in FIG. **4**, magnetic data bits d**0**-d2 are arranged in a single track. A set of fixed-position write heads **404**, **406**, and **408** respectively write and rewrite magnetic data bits d**0**-d**2**. A moving, scanning read head **410** in a legacy magnetic card reader is used to read out the data written.

[0039] Parts of magnetic data storage array **400** can be implemented with MEMS technology. In general, MEMS is the integration of mechanical elements, sensors, actuators, and electronics on a common substrate using microfabrication technology. Electronics devices are typically fabricated with CMOS, bipolar, or BICMOS integrated circuit processes. Micromechanical components can be fabricated using compatible "micromachining" processes that selectively etch away parts of a processing wafer, or add new structural layers to form mechanical and electro-mechanical devices.

[0040] In the present case, MEMS technology can be used to fabricate coils that wind around Permalloy magnetic cores with gaps to produce very tiny magnetic transducer write heads. For example, a magnetic transducer write head that would be useful in the payment card **100** of FIG. **1** would have a gap length of 1-50 microns, a core length of 100-250 microns, a write track width of 1000-2500 microns, and a read track width of 1000 microns. Nickel-iron core media permeability would be greater than 2000, and cobalt-platinum or gamma ferric oxide media permeability would be greater than 2.0, and the media coercivity would be a minimum of 300 Oe.

[0041] A parallel array static MEMS (S-MEMS) device is a magnetic transducer which will allow information to be written in-situ on the data tracks of a standard form factor magnetic stripe card. In a practical application, an array of twenty-five individual magnetic bit cells can be located at one end of an ISO/IEC/IEC 7811 standard magnetic media. Such a stripe includes some permanent encoding, as well as a region in which data patterns can be written by arrays of magnetic heads attached to a low-coercivity magnetic stripe.

[0042] Each cell of such parallel array is independently electronically addressed. Write transducer current may flow in one direction or the other, depending on the desired polarity of the magnetic data bits. The magnetic stripe transaction reader operates by detection of magnetic domain transitions within an F2F scheme typical of such cards and, therefore, magnetic domain reversal is not necessary. A prototype write head included a high permeability NiFe core with electroplated windings of copper wires. For example, a useful write head has a z-dimension (track width) of 1000-2500 microns, a width of 100 microns in the x-direction, and a height in the y-direction of approximately 20 microns. There are four coil turns around each pole piece, for a total of eight. The cross sectional area of the coil was estimated at four microns square, with a three micron spacing. Total length in the x-direction, including core and coils, was 150 microns, and about a ten micron spacing between adjacent magnetic cells.

[0043] Transaction process embodiments of the present invention embed an algorithm with unique user data in a cryptoprocessor. For example, a method for a transaction process embeds an algorithm that encodes unique user data in a cryptoprocessor. It requests a new unique transaction encoding to be issued by using the cryptoprocessor to process the algorithm and to generate a data suited to a card-acceptance system pre-processing requirements. A conventional transaction infrastructure and server can then be used to derive from the number the unique user data. The new unique transaction encoding can be communicated to the conventional transaction infrastructure and server by a smart card contact or proximity connection. The new unique transaction encoding can be communicated to the conventional transaction infrastructure and server by a reprogrammable magnetic stripe on a card read by a reader. Such is useful in validating and approving point-of-sale financial transactions.

[0044] The following several paragraphs are repeated here for convenience from parent case, U.S. Pat. No. 7,044,394, issued May 16, 2006, titled PROGRAMMABLE MAGNETIC DATA STORAGE CARD.

[0045] In general, a predictive algorithm is used that includes personal information about the user as some of its factors. This then generates a unique number that is not sequential and cannot be guessed. For example, such can be included as a card validation code value now in common use. A payment processing center keeps track of this usage-counter data field, and will not authorize transaction requests that come out of sequence. For example, as can occur from a magnetic clone of a card that has been skimmed and tried later. A card-swipe detector embedded in the plastic card detects each use in a POS terminal, and it signals an internal microcomputer which changes data bits sent to the write heads. Once scanned by the POS terminal or other reader, the payment card can also disable any reading of the user account data for a short fixed period of time.

[0046] In some embodiments of the present invention, the payment card **100**, **200** is constructed to provide an automatically incrementing usage-number that can be forwarded in an approval request message to a validation processing center. The validation processing center stores the last incrementing usage-number used in a valid transaction and any new usage-number used must be greater. If it is not, an out-of-sequence transaction has been detected that is probably the result of card skimming and fraud. The transaction request is subsequently denied.

[0047] Alternatively, such dynamic number may be a unique algorithm composed of two or more factors that may include the user's billing address numbers and social security number or card numbers that provide unpredictable results not in a sequential manner. The Assignee refers to such commercial analysis methods and devices with its trademark, Dynamic Numerical Analysis (DNA™).

[0048] One way to implement a user validation test is with a dynamic numerical analysis (DNA). An algorithm is implemented that fetches a last used valid number from a private database, and compares this with the sequence number now being attempted.

[0049] In other embodiments of the present invention, the payment card **100**, **200** is constructed to provide a sort of PIN value that can be forwarded in an approval request message to a validation processing center. In one instance, unique-number generator **204** internal to the card is used to supply a value in a discretionary field of Track-2, or the card validation code (CVC) field. Such unique number is generated by an algorithm that uses as its factors the user's social security number, the user's billing address, etc.

[0050] The payment card **100**, **200** can also be constructed to provide user account data for only limited times. For example, a PIN pad integrated on the payment card **100**, **200** can require a user PIN number to be entered before card magnetic data **202** will present itself for swiping in the card reader **201**. A lack of card magnetic data **202** simply looks to card reader **201** as a defective card, and denies the transaction. No hardware or software changes are needed in the card reader **201** to work with payment card **100**, **200**. Therefore, card reader **201** can be an already preexisting conventional device.

[0051] The card reader **201** performs various magnetic data operations and checks on the card magnetic data **202**. For example, a longitudinal redundancy code (LRC) check that helps assure a valid read of all the data has been made. Once the card reader **201** has determined the card magnetic data **202** is good, an approval request message is sent to a card acquirer. Such message includes the user account number, dollar amount of the transaction, and merchant identification (ID). It further contains special transaction serializing information to detect skimming and other fraud.

[0052] A validation processing center provides regional high-speed network servers that are often operated by third parties and not the issuing banks. The validation processing center checks to see if the user card **100**, **200** is not stolen or lost, and other first level account validation. It may also have cached some information from an issuing bank about this user account if the account has been processed before very recently. A card acquirer approval message is sent to an issuing bank. It also includes the user account number, dollar amount of the transaction, and merchant identification (ID). The user account is checked to see if adequate funds are available, and if so, sends an authorization message. A reconciliation of the user account is made and the merchant's account is credited with a day or two. The card acquirer records the issuing-bank authorization and forwards an approval message. The merchant point-of-sale card reader displays the approval and an authorization code, and the transaction is completed.

[0053] Although particular embodiments of the present invention have been described and illustrated, such is not intended to limit the invention. Modifications and changes will no doubt become apparent to those skilled in the art, and it is intended that the invention only be limited by the scope of the appended claims.

The invention claimed is:

1. A three-mode payment card configured in a standardized credit card format equivalent to ISO/IEC-7810, and having:

a plastic card body in which all the other elements are disposed;

a contact interface with surface contacts and providing for communication of encoded bank and user information with a contact-type smartcard reader in a first mode;

a wireless interface with an antenna and providing for contactless communication of encoded bank and user information with a contactless-type smartcard reader in a second mode;

a dual-input crypto-processor for supporting contact-type smart card communication equivalent to ISO/IEC-7816 through the contact interface, and for also supporting contactless-type smart card communication equivalent to ISO/IEC-14443 through the wireless interface;

and characterized by:

a magnetic stripe with a magnetic array interfaced to the dual-input crypto-processor, and that provide for magnetic presentations in parallel that mimic a conventional legacy magnetic stripe encoded with bank and user information to a magnetic card reader in a third mode;

a magnetic recording serially accessible to a longitudinally moving read head on a front side of the magnetic stripe that includes at least one dynamic data bit controlled by said magnetic array;

a data generator and a data receptor for receiving an initial programming of personalization data from a card issuer, bank agency or manufacturer, and for outputting through the magnetic array a number of programmable data bits that are combined in a string with a number of permanent data bits;

a programmable interface controller (PIC) interfaced to the dual-input crypto-processor through the contact interface;

an input device for accepting information solicited from a user and providing it to the PIC; and

an electronic display connected to present text messages from the PIC to said user.

2. The payment card of claim **1**, further comprising:

a component providing for user authentication based in-part on said information entered through the input device;

3. The payment card of claim **1**, wherein:

the input device includes a biometric sensor for collecting physical characteristics of a user that are thereafter useful by the PIC in an authentication of said user.

4. The payment card of claim **1**, wherein:

the input device includes a biometric sensor for collecting at least one of a fingerprint or signature of a user that are thereafter useful by the PIC in an authentication of said user.

5. The payment card of claim **1**, further comprising:

an algorithm with data unique to said user and embedded in the dual-input crypto-processor, wherein a new unique transaction encoding is transmittable through the wireless, contact, and magnetic interfaces that permits a transaction infrastructure and server to derive a unique user data that is useful in validating and approving point-of-sale financial transactions involving the payment card.

6. The payment card of claim **1**, wherein:

the PIC does not store more than one digit of a user password at a time, and sends each digit as it is received on to the contact interface and the dual-input crypto-processor for verification.

7. The payment card of claim **6**, wherein:

the PIC does not store a whole user password at any time.

8. The payment card of claim **1**, wherein:

a portion of a complete financial account number of the user is encoded with said permanent data bits.

9. The payment card of claim **1**, wherein:

the data generator provides for a subsequent obfuscation of a financial account number being presented in whole by rewriting said at least one dynamic data bit controlled by said magnetic array.

10. The payment card of claim **1**, further comprising:

a predictive algorithm that includes personal information about the user in some of its factors, and that generates a unique number that is not sequential and cannot be predicted without knowing the algorithm and the seed value, and wherein a payment processing center will not authorize transaction requests that come out of sequence.

11. The payment card of claim **10**, further comprising:

detectors connected to signal the PIC when a reading of bank and user information in the magnetic recording has occurred.

12. The payment card of claim **1**, further comprising:

an on-board electrical generator connected to power the payment card as needed.

13. The payment card of claim **1**, further comprising:

a piezoelectric generator connected to charge a battery that powers the payment card as needed.

14. A three-mode payment card having:

means for providing communication of encoded bank and user information with a contact-type smartcard reader in a first mode;

means for providing communication of encoded bank and user information with a contactless-type smartcard reader in a second mode;

and characterized by:

means for providing magnetic presentations in parallel that mimic a conventional legacy magnetic stripe encoded with bank and user information to a magnetic card reader in a third mode;

means for providing a magnetic recording serially accessible to a longitudinally moving read head on a front side of the magnetic stripe that includes at least one dynamic data bit controlled by said magnetic array;

means for receiving an initial programming of personalization data from a card issuer, bank agency or manufacturer, and for outputting a number of programmable data bits that are combined in a string with a number of permanent data bits;

means for accepting information solicited from a user; and

means for presenting text messages from to said user.

15. A payment card configured in a standardized credit card format equivalent to ISO/IEC-7810, and having:

a plastic card body in which all the other elements are disposed;

at least one of a contact interface with contact-type smart card communication equivalent to ISO/IEC-7816, and a wireless interface with an antenna providing for contactless-type smart card communication equivalent to ISO/IEC-14443;

a crypto-processor for supporting smartcard communication through either of said contact and wireless interfaces;

and characterized by:

a data generator and a data receptor for receiving an initial programming of personalization data from a card issuer, bank agency or manufacturer, and for encoding bank and user information for output by either of said contact and wireless interfaces with sequenced portions that can be expected by the card issuer;

a programmable interface controller (PIC) interfaced to the crypto-processor; and

an electronic display connected to present text messages from the PIC and the crypto-processor to said user.

16. The payment card of claim **15**, further comprising:

a device for automatically incrementing a value in a sequence that can be forwarded in an approval request message to a validation processing center, wherein changing values used in transactions must belong to an expected sequence in order to be valid.

17. The payment card of claim **15**, further comprising:

a magnetic stripe with a magnetic array interfaced to the crypto-processor, and that provide for magnetic presentations in parallel that mimic a conventional legacy magnetic stripe encoded with bank and user information to a magnetic card reader in a third mode; and

a magnetic recording serially accessible to a longitudinally moving read head on a front side of the magnetic stripe that includes at least one dynamic data bit controlled by said magnetic array;

wherein, the data generator and data receptor further provide for outputting through the magnetic array a number of programmable data bits that are combined in a string with a permanent data bits.

* * * * *