

(19) World Intellectual Property Organization
International Bureau



(43) International Publication Date
4 September 2008 (04.09.2008)

PCT

(10) International Publication Number
WO 2008/106561 A2

(51) International Patent Classification:
G06K 5/00 (2006.01)

(74) Agents: **HALL, David, A.** et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, 8th Floor, San Francisco, CA 94111-3834 (US).

(21) International Application Number:
PCT/US2008/055196

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DO, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT, HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP, KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD, ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RS, RU, SC, SD, SE, SG, SK, SL, SM, SV, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, ZA, ZM, ZW.

(22) International Filing Date:
27 February 2008 (27.02.2008)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
11/680,592 28 February 2007 (28.02.2007) US

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, NO, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

(71) Applicant (for all designated States except US): **VISA U.S.A. INC.** [US/US]; P.O. Box 8999, San Francisco, CA 94128 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **DIXON, Philip, B.** [US/US]; 7389 Juncus Court, San Diego, CA 92129 (US). **HAMMAD, Ayman** [US/US]; 6981 Corte Mercado, Pleasanton, CA 94566 (US). **EL-AWADY, Khalid** [US/US]; 1938 Montecito Avenue, Apt. 2, Mountain View, CA 94043 (US).

Published:

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

(54) Title: VERIFICATION OF A PORTABLE CONSUMER DEVICE IN AN OFFLINE ENVIRONMENT

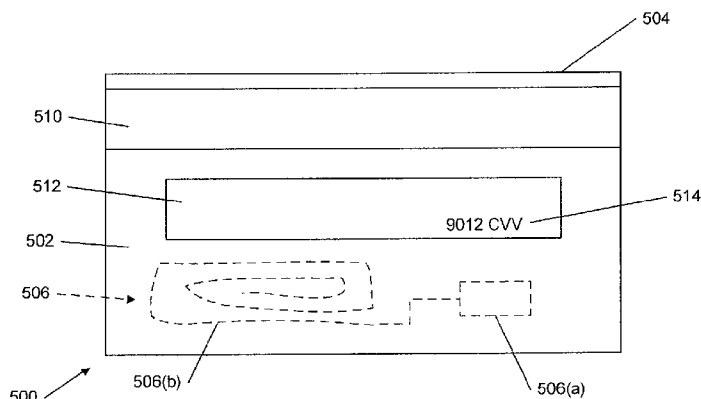


FIG. 5

(57) Abstract: A portable consumer device includes a base, and a computer readable medium on the base. The computer readable medium comprises code for an issuer verification value and a supplemental verification value. The issuer verification value is used by an issuer to verify that the portable consumer device is authentic in an on-line transaction and the supplemental verification value is used to verify that the portable consumer device is authentic in an off-line transaction.

VERIFICATION OF A PORTABLE CONSUMER DEVICE IN AN OFFLINE ENVIRONMENT

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This application claims priority to U.S. Patent Application 11/680,592 filed
5 February 28, 2007 entitled "Verification of Portable Consumer Device in an Offline
Environment" by A. Hammad et al. The contents of the patent application are incorporated
herein by reference in its entirety for all purposes. The contents of the patent applications
entitled "Fraud Prevention for Transit Fare Collection" to A. Hammad et al. Application No.
11/680,589 filed February 28, 2007 and "Authentication of a Data Card Using a Transit
10 Verification Value" by A. Hammad et al. Application No. 11/680,594 filed February 28,
2007 and "Bank Issued Contactless Payment Card Used in Transit Fare Collection" to A.
Hammad et al. U.S. Patent Application No. 11/566,614 filed December 4, 2006 and
"Mobile Transit Fare Payment" to A. Hammad et al. U.S. Patent Application No.
11/536,296 filed September 28, 2006 are incorporated herein by reference in their entirety
15 for all purposes.

BACKGROUND

[0002] In a conventional consumer card payment transaction, a cardholder presents a
merchant with a portable consumer device such as a credit card to pay for goods or services.
The processing of the transaction involves the merchant, an acquirer, a payment processing
20 network, and a card issuer. The merchant initiates online processing and forwards an
authorization request message to the acquirer, through the payment processing network, and
to the issuer. The issuer verifies that the card number, transaction amount, and other
information are valid and returns an authorization response message for the transaction back
to the merchant. A variety of fraud prevention measures are used by issuers to guard
25 against the unauthorized (or wrongly authorized) use of such cards.

[0003] Fraud prevention measures include a Cardholder Verification Value (CVV), which
comprises a three-digit code that is stored within a magnetic stripe data (MSD) region of the
card when the issuer provides the card for personalization. The issuer maintains a database
of the CVV data for the issued cards and can therefore check an incoming request for

authorization against the CVV data maintained at the issuer for the card in question. The issuer can safeguard the CVV data to ensure that such data is not shared outside of the issuer, thereby maintaining an increased level of security against fraud and counterfeit cards.

- 5 **[0004]** Under some situations, offline processing using a payment card is desirable. For example, transit fare processing from payment cards is typically conducted offline, because of transaction speed requirements at transit fare collection devices such as subway turnstiles or bus fareboxes. For transit transactions, thirty to forty-five customers (passengers) are processed per minute, so there is insufficient time for the merchant (the transit system) to go
10 online to the issuer for transaction authorization. Moreover, such transactions typically utilize some form of contactless card for payment that does not require physical contact between the card presented for payment and the transit fare collection device of the transit system. In these situations, some form of offline card authentication is desirable to prevent potential counterfeit card attacks and the potential organized fraud.
- 15 **[0005]** In this discussion, "contactless cards" for payment systems will include contactless "smart" cards and also contactless smart chips. A smart card is generally defined as a pocket-sized card (or other portable consumer device) that is embedded with either a microprocessor and one or more memory chips, or as one or more memory chips with non-programmable logic. The microprocessor-type smart card typically can implement certain
20 data processing functions, such as to add, delete, or otherwise manipulate information stored in a memory location of the smart card. In contrast, the memory-chip-type card (for example, a pre-paid phone card) can only act as a file to hold data that is manipulated by the reading device to perform a predefined operation, such as debiting a charge from a pre-established balance held in the memory or secure memory. Smart cards, unlike magnetic
25 stripe cards (such as conventional credit cards), can implement a variety of functions and contain a variety of types of information on the card. Therefore, in some applications they do not require access to remote databases for the purpose of user authentication or record keeping at the time of a transaction. A smart chip is a semiconductor device that is capable of performing most, if not all, of the functions of a smart card, but may be embedded in
30 another device.

[0006] A contactless smart card is a smart card that incorporates a means of communicating with the card reader or terminal without the need for direct contact. Thus,

such cards may effectively be "swiped" by passing them close to the card reader or terminal. Such contactless smart cards typically communicate with the card reader or terminal using RF (radio-frequency) technology, wherein proximity to an antenna causes data transfer between the card and the reader or terminal. Contactless smart cards have found uses in banking and other applications, as it may not be necessary to remove them from one's wallet or pocket in order to complete a transaction. Furthermore, because of the growing interest in such smart cards, standards have been developed that govern the operation and interfaces for contactless smart cards, such as the ISO 14443 standard. A variety of financial transactions, such as retail payment and transit fare collection, have adopted the ISO 14443 standard for contactless smart cards.

[0007] As noted above, an MSD area of a payment card can be used to store CVV data and the like to protect against fraudulent use in consumer transactions. In a contactless smart card, data for an additional, separate payment application, such as a transit application, might be stored in the card and might be feasible for performing offline authentication processing. The additional transit application data stored in the MSD area would require specialized readers that can detect and execute the offline-payment transit application. This would require additional effort on the part of the issuer to install and manage such applications, placing a burden on the issuer that may prevent widespread adoption of the solutions.

[0008] From the discussion above, it should be apparent that there is a need for transaction processing that can perform authorization operations in an offline transaction processing environment. Embodiments of the present invention satisfy this need.

SUMMARY

[0009] One embodiment of the invention is directed to a method of processing a transaction, in which data is received from a portable consumer device at a reader, wherein the portable consumer device stores an issuer verification value associated with an issuer and a supplemental verification value, and wherein the supplemental verification value is verified using an offline processing system. The supplemental verification value is then processed at the reader, and the transaction is authorized if the processed supplemental verification value indicates that the portable consumer device is authenticated. A contactless smart card does not require a separate application area for storing application

data in connection with the offline payment processing, so that specialized card readers for reading from a separate offline application area are not required. This facilitates performing authorization operations in an offline transaction processing environment.

[0010] Another embodiment of the invention is directed to a method of providing a portable consumer device, the method comprises receiving supplemental verification value associated with an offline processing system; and storing the supplemental verification value and issuer verification value in the portable consumer device.

[0011] Another embodiment of the invention is directed to a portable consumer device comprising a base, and a computer readable medium on the base, wherein the computer readable medium comprises code for an issuer verification value and a supplemental verification value, wherein the issuer verification value is used by an issuer to verify that the portable consumer device is authentic in an on-line transaction and wherein the supplemental verification value is used to verify that the portable consumer device is authentic in an off-line transaction.

[0012] Another embodiment of the invention is directed to a reader configured to: receive data from a portable consumer device at a reader, wherein the portable consumer device stores an issuer verification value associated with an issuer and a supplemental verification value, wherein the supplemental verification value is verified using an offline processing system; process the supplemental verification value at the reader; and authorize the transaction if the processed supplemental verification value indicates that the portable consumer device is authenticated.

[0013] Other objects and advantages of the present invention will be apparent to one of ordinary skill in the art upon review of the detailed description of the present invention and the included figures.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] Figure 1 is a depiction of a portable consumer device and processing system constructed in accordance with the present invention.

[0015] Figure 2 is a flow diagram representation of processing in the Figure 1 system.

[0016] Figure 3 is a flow diagram representation of a more specific method of processing in accordance with the present invention, using a supplemental verification value, which is a transit card verification value.

[0017] Figure 4 is a depiction of the portable consumer device illustrated in Figure 1.

5 [0018] Figure 5 is an illustration of a portable consumer device of Figure 4 comprising a contactless smart card constructed in accordance with the invention.

[0019] Figure 6 is a representation of the Track 1 and Track 2 data of the Figure 5 contactless payment card with the supplemental verification value data.

DETAILED DESCRIPTION

10 [0020] In embodiments of the invention, a portable consumer device (e.g., a contactless payment card or payment token device) includes a supplemental verification value that can be validated at a reader (e.g., a payment collection reader) that is offline. The supplemental verification value is preferably a transit verification value that is used in a transit environment. If the supplemental verification value is on a payment card, it may be referred to as a "supplemental card verification value." The supplemental verification value may be
15 in the form of a multi-digit number (e.g., a three-digit number) or some other data string.

[0021] If the portable consumer device is provided as a payment card, then the supplemental verification value can be stored in a computer readable medium (e.g., a memory chip, magnetic stripe media, etc.) of the payment card, along with a conventional
20 card verification value (which may be referred to as an "issuer verification value" in some cases), which is used for conducting typical online financial transactions. Thus, a portable consumer device according to an embodiment of the invention may include both an issuer verification value for online transactions and a supplemental verification value for offline transactions. The issuer verification value is preferably not used for offline transactions and
25 the supplemental verification value is not used for online transactions. In addition, the supplemental verification value as well as the issuer verification value may be static (will not change in normal operation after issuance of the portable consumer device) or may be dynamic (can change over time following issuance).

[0022] As used herein, an "online" transaction generally includes a transaction that would
30 need an electronic authorization response from the issuer before the transaction could be

conducted. An "offline" transaction is a transaction that does not require an issuer's response over an electronic communication medium before the transaction is conducted. An example of an offline transaction includes an attempt to gain access to a transit system, such as to a subway facility through a turnstile at a subway station. Another example of an offline transaction is an attempt to gain entry to a facility such as a building or venue through a closed gateway or door. A transaction may be considered "offline" if the decision as to whether or not the user may pass through the turnstile is made at the turnstile or at a computer that is proximate to the turnstile (e.g., at the same locale, such as at the same subway station), and the decision as to whether or not the user may pass through the turnstile is not made by the issuer of the portable consumer device. At some point after the user has gained access to the facility, the turnstile or the computer connected to the turnstile will communicate with the issuer so that the issuer may debit the account of the user for the entry or use of the facility.

[0023] In the context of a payment card, validation of a supplemental card verification value provides a mechanism for verification of the card authenticity at the time of use. If the card can be verified as authentic, then the potential for counterfeiting of cards for use in the offline transaction environment is reduced. This advantageously helps prevent runaway fraud. In addition, as will be explained in more detail below, the supplemental card verification value may be stored in a traditional magnetic stripe data format along with an issuer card verification value. Specialized security applications need not be stored on the portable consumer device, and can be used with conventional payment processing systems that process magnetic stripe credit card or debit card transactions. Major modifications to such systems are not needed to allow embodiments of the invention to operate. Lastly, the user of the portable consumer device benefits since the user may use the portable consumer device for both offline and online transactions.

[0024] Embodiments of the invention are described in further detail below with reference to the Figures.

[0025] Figure 1 is a depiction of a portable consumer device 102 and a processing system 103 constructed in accordance with the present invention. Although specific components are shown in Figure 1, systems according to embodiments of the invention may include more or less components than are shown in Figure 1. For example, although two separate

blocks are shown for the issuer 112 and the acquirer 110, it should be understood that a single organization may act as both an issuer and an acquirer in some cases.

[0026] The portable consumer device 102 according to embodiments of the invention may be in any suitable form for the processing described herein. For example, the portable consumer device can be hand-held and compact so that it can fit into a consumer's wallet and/or pocket (e.g., pocket-sized). Such portable consumer devices may include smart cards, ordinary credit or debit cards (with a magnetic strip and without a microprocessor), a token or keychain device (such as the Speedpass™ device commercially available from Exxon-Mobil Corp.), and the like. Other examples of portable consumer devices that can be constructed in accordance with the invention include consumer electronic devices such as cellular phones, personal digital assistants (PDAs), pagers, and the like. Other examples of portable consumer devices 102 include payment cards, security cards, access cards, smart media, transponders, and the like.

[0027] For purposes of illustration, embodiments of the invention are described in the context of contactless payment cards, but embodiments of the invention are not limited thereto, as noted above. Embodiments of the invention are configured for offline processing of transactions such as payment transactions, access transactions, and the like. For example, the supplemental verification value could be used for a non-financial transaction such as gaining access to a secure building or a venue where a ticket has already been prepaid. In the context of this description, the contactless card will be described in connection with readers of a transit fare collection system. Other offline systems in which the embodiments are useful include venue entrance locations, turnstiles, building entrances, vending machines, secured access areas, and the like.

[0028] In embodiments of the invention, the contactless payment card typically communicates with a reader that is part of a transit system fare collection mechanism using a short range communication method, such as a near field communications (NFC) capability. Examples of such NFC technologies include ISO standard 14443, RFID, Bluetooth™ and infra-red communications methods. A contactless payment card typically comprises a base and a computer readable medium. The computer readable medium can include logic circuitry and an antenna for contactless communication. If the payment card is a smart card, then the card may include a microprocessor to perform smart card functions. The computer readable medium may be in the form of a memory chip, magnetic stripe

media, and the like. Some contactless payment cards may also have both an antenna for contactless-type transactions and a magnetic stripe or electrical contacts for contact-type transactions.

[0029] Referring to Figure 1, processing in accordance with the invention is initiated when the portable consumer device 102 is presented for use and is read by the reader 104, which may be a contactless reader at a fare collection or venue entrance point. In the case of the illustrated portable consumer device 102, the data stored on the portable consumer device includes an issuer verification value (e.g., a CVV) for use in authenticating the portable consumer device in online transactions, and includes a supplemental verification value that is used to verify the authenticity of the portable consumer device in offline transactions. The offline transactions may or may not be offline payment transactions.

[0030] The supplemental verification value is received by the reader 104 and the transaction is authorized if the processed supplemental verification value indicates that the portable consumer device 102 is authenticated. The reader operates in an offline mode, so that authentication can occur at minimal intervals, such as are needed in the transit fare collection environment and other offline operating modes. The reader 104 may also include a processor (not shown) and a computer readable medium (not shown). It may also comprise a single device, or multiple interconnected devices. In embodiments of the invention, the authentication of the portable consumer device 102 may take place solely at the reader 104. In another embodiment, the authentication of the portable consumer device 104 could even take place at the transit system central computer 108, if appropriate network communication or speed requirements are met. Generally, the authentication decision takes place at the same locale or site (e.g., the same train station, the same store, etc.) as the reader 104. In both of the above examples, however, the authentication decision in an "offline" transaction is not conducted by the issuer 112 before the user of the portable consumer device 102 is able to perform the requested transaction.

[0031] Although the reader 104 in this example is a contactless reader, it is understood that a contact-based reader (e.g., a magnetic stripe reader with a card-receiving slot) could be used in other embodiments of the invention.

[0032] In a typical transaction, the portable consumer device 102 interacts with the reader 104. The reader 104 receives magnetic stripe track data including Primary Account Number (PAN) information, expiration date, service codes, the supplemental verification

value, and the like associated with the portable consumer device 102. The reader 104 (which may be considered to be a transit fare collection device in some cases) may also have any encryption keys and associated algorithms for processing the supplemental verification value on the card, and thus may authenticate the portable consumer device 102 at the time of the transaction with no online processing. If the PAN and expiry date information are validated at the reader 104 and the device is authenticated, then the user presenting the portable consumer device 102 is allowed access to conduct the transaction (e.g., pay a fare and gain entry into a transportation system).

[0033] In preferred embodiments, after the authentication of the portable consumer device 102, and after the transaction is conducted by the user of the portable consumer device 102, the reader 104 can forward the PAN information (or a proxy account number) over a transit system data network 106 to the transit central computer 108 along with the time, date, and location of the transaction. The transit central computer can perform a fare calculation based on the history of transactions for the portable consumer device 102 (which is uniquely identified by the PAN) along with the fare policy as defined by the transit agency.

[0034] Payment processing may be performed as defined by the transit agency. Payment models implemented with the card can include a variety of schemes, such as pay-as-you-go, one transaction at a time; aggregation of many transactions into an aggregated amount based on time or value; and pre-pay accounting, where a proxy account is created and is reduced by each transaction amount until a replenishment of the proxy account is required based on time or value. After the payment processing is complete, the transit agency computer 108 processes the payment total through the acquirer 110 and a payment processing network 111 (e.g., VisaNet™) for approval or decline by the issuer 112. Any of the transit system data network 106, the transit system central computer 108, the acquirer 110, the payment processing network 111, and the issuer 112, may have suitable computational apparatuses and computer readable media suitable for performing any of the functions described herein.

[0035] Figure 2 is a general flow diagram representation of the transaction processing that can be performed by the system shown in the Figure 1. As noted above, the processing conducted by the system using the supplemental verification value can be performed without making any changes to the data format specifications for contactless payment using Magnetic Stripe Data (MSD) rules, such as the ISO 7813 standard. These specifications are based on the use of Track 1 and Track 2 data to deliver the cardholder data to the point of

sale. The majority of payment cards used today are configured in accordance with a magnetic stripe data format for financial transaction cards. Although contactless transactions do not use a magnetic stripe, data from a contactless portable consumer device may still be considered "magnetic stripe data" because the data can be used with
5 conventional processes and systems that process data from credit and debit cards that use magnetic stripes to store information.

[0036] The system shown in Figure 1 system utilizes data fields of the Track 1 and Track 2 to store the supplemental verification value. Track 1 ("International Air Transport Association") stores more information than Track 2, and contains the cardholder's name as
10 well as account number and other discretionary data. This track is sometimes used by the airlines when securing reservations with a credit card. Track 2 ("American Banking Association,") is currently most commonly used. This is the track that is read by ATMs and credit card checkers. It contains the cardholder's account, encrypted PIN, plus other discretionary data.

15 [0037] The portable consumer device constructed in accordance with the present invention provides a mechanism for insertion of the supplemental verification value into standard track data to be validated at the reader. Thus, the first operation represented in Figure 2 by box 202 is to generate the supplemental verification value for offline processing.

20 [0038] In one embodiment, an encryption algorithm is used to create and decipher the supplemental verification value. A suitable encryption algorithm can utilize one or more encryption keys, and may be of either symmetric (e.g. DES or 3 DES) or asymmetric type (e.g. public key infrastructure). At box 204 of Figure 2, the encryption algorithms and encryption keys associated with the supplemental verification value are generated and
25 provided to the bank or other business institution that will personalize the card. Card personalization devices at the payment card personalization facility will load the appropriate supplemental verification value to the portable consumer device. The keys and algorithms are also sent to the reader so that the reader can decrypt the supplemental verification value when it is received.

30 [0039] In the illustrated embodiment, the TCVV data includes a full or partial cryptogram that could be based on a system-wide key, or unique card values and encryption keys. The use of encryption algorithms and keys may include symmetric (i.e. triple DES) or public

key infrastructure (i.e. RSA). The issuer of the card places this data into the track data of the transit MSD application at the time of card personalization. In the case of public key infrastructure, additional data elements may be necessary and may be stored outside the track data and read by the transit contactless reader along with the track data during the transit fare transaction. The contactless reader or transit fare device will have the encryption keys and algorithm for the TCVV data, and may then authenticate the TCVV value at the time of the transaction. The authentication can take place in the short time interval necessary for processing in the transit and venue access environment, as described above.

[0040] In one embodiment, the supplemental verification value is placed into the standard Track 1 or Track 2 data elements within the primary MSD application. A variety of Track 1 and Track 2 positions can be used for storing the supplemental verification value. For example, positions 25 to 29 of the Track 2 data fields that would normally indicate PIN verification information may be used for storing the supplemental verification value. In another alternative, Track 1 issuer discretionary data locations may be used for this purpose. The exact positions of the code within the track data will be standardized so that the issuer and merchant transit agency (or other entity) will know where to load or retrieve the data. Alternatively, other data elements may be located outside of the Track 1 and Track 2 data fields, such as in supplemental data fields of the portable consumer device. The supplemental verification value also may comprise data elements that are split and stored in distributed locations so that the value is partially stored in track data (Track 1, or Track 2, or both) and is partially stored outside of the track data.

[0041] The supplemental verification value is also provided to the reader, at box 206. The reader will authenticate the contactless portable consumer device at the time of use. Thus, the supplemental verification value can be used in an offline transaction authorization process.

[0042] The operation at box 206 is to actually issue the portable consumer device with the supplemental verification value. Typically, the issuer mails the contactless portable consumer device to the user. Once received and activated, the card may be used in conventional online financial transactions using the issuer verification value (e.g., CVV) that is also stored on the portable consumer device. It may also be used in an offline

transaction as described herein and illustrated in Figure 1, such as the transit fare collection processing.

[0043] In accordance with the offline authorization processing, the contactless payment card may be presented at a reader, represented by box 208. At the reader, the reader may receive information including the supplemental verification value and may receive other information such as the PAN, expiry date, service code, and the like.

[0044] After the track data is read by the transit fare collection device, at box 210, the reader will perform offline authorization processing and will utilize the supplemental verification value to determine if the portable consumer device is authentic. This provides a mechanism for authentication at the reader that provides for the ability to identify counterfeit cards that do not have the proper supplemental verification value. A transaction is authorized by the transit fare collection device if the processed supplemental verification value indicates that the portable consumer device is authentic. For example, authentication may include calculating a value at the reader as determined by appropriate keys and algorithms for the supplemental verification value read from the device, and comparing the calculated value with the value read from the card such that, if the calculated value matches an authentication or verification value, the portable consumer device is authenticated.

[0045] Figure 3 is a flowchart illustrating a more specific method of processing using a supplemental verification value in accordance with the invention. In this more specific method, the portable consumer device is a contactless card configured for transit application (i.e., a transit card) and the supplemental verification value is a "transit card verification value" or TCVV.

[0046] At the Figure 3 box numbered "1", an algorithm is determined and at box "2" is sent or provided to a bank card personalization center and to a transit system with which the transit card will be used. The algorithm is used to create and decipher a supplemental verification value that is loaded into the track data of the contactless payment card or loaded into other data components outside of the track data. The algorithm utilizes one or more encryption keys, and may be of either symmetric (i.e. DES or 3 DES) or asymmetric type (i.e. public key infrastructure). Thus, at the box "2", the keys and algorithms are transmitted to the devices at the bank that will personalize the supplemental verification value onto the card, and also to the transit fare devices that will validate the supplemental verification

value at the time of use. Based on predetermined key management processes at "2", the reader will be able to identify the proper algorithms and keys to use.

[0047] At the box "3" of Figure 3, the bank personalization system will load the appropriate supplemental verification value to the transit card based on the algorithm and keys. This data may be placed into the standard Track 1 or Track 2 data elements within the primary MSD application area, or can be placed in other data components outside of the track data, or can be placed in a combination of all. In one embodiment, positions 25 to 29 of the Track 2 data that would normally indicate PIN verification information may be used for the transit application. In another embodiment, Track 1 issuer discretionary data locations may be used for the transit application data. As noted above, the data can be outside of the track data, such as in data tags stored elsewhere, or the data can be split up and portions can be stored in multiple locations. The exact positions of the supplemental verification value within the track data or within the other data components or data tags outside of the track data will be standardized so that the issuer and transit agency will know where to load or retrieve the supplemental verification value.

[0048] At box "4" of Figure 3, the issuer mails the card to the cardholder as normal for retail use. Once received and activated, the card may also be used in transit. The transit patron (the cardholder) may use the contactless component of the card in any transit system that is enabled to read and react to the contactless payment data, and specifically the TCVV code that has been loaded onto the card at box "3". At box "5" of Figure 3, at the transit fare device, the card is read by the reader. The reading process reads the MSD application that provides payment track data including PAN, expiry date, service code, and so forth. In addition, the TCVV code will be included in specified data positions of the portable consumer device so it can be read. Once the verification value is read by the transit fare reader, the reader will utilize the keys and algorithm for validation of the TCVV code. That is, the supplemental verification value is processed by identifying an appropriate key and algorithm, and calculating at the reader a value corresponding to the portable consumer device, and comparing the calculated value to the supplemental verification value received from the portable consumer device. A calculated value that matches or agrees with the received value indicates authentication. This provides a mechanism for card authentication by the reader that provides the ability to detect counterfeit cards that will not have the proper TCVV value for authentication.

[0049] Figure 4 illustrates a portable consumer device 400 constructed in accordance with the present invention. The device 400 can be provided in a variety of forms. For example, the portable consumer device can be hand-held and compact so it can fit into a consumer's wallet and/or pocket (e.g., pocket-sized). Suitable portable consumer devices may include smart cards, ordinary credit or debit cards (with a magnetic strip and without a microprocessor), a keychain device (such as the Speedpass™ device commercially available from Exxon-Mobil Corp.), and the like. Other examples of portable consumer devices that can be constructed in accordance with the invention include wireless cellular telephones, personal digital assistants (PDAs), pagers, payment cards, security cards, access cards, smart media, transponders, and the like, configured for compatible operation in the processing illustrated in Figure 1.

[0050] Figure 4 shows that the portable consumer device 400 includes a primary (issuer) verification value 402 for online issuer verification and a supplemental verification value 404 for the offline processing described herein. The portable consumer device also includes interface processing components 406 such as processors and the like for proper functioning and data exchange. For example, a portable consumer device 400 comprising a transit smart card will include interface components that enable communication with offline readers of the transit system and will include the appropriate supplemental verification value for successful operation. A portable consumer device 400 such as a token or keychain device will include interface components for communication with the offline token/keychain reader and will include the appropriate supplemental verification value. A portable consumer device 400 such as a wireless telephone will include interface components for communication with the offline reader and will include the appropriate supplemental verification value for successful operation with the offline reader and associated processing system, along with components for the wireless telephone operation.

[0051] Figure 5 shows an embodiment in which the portable consumer device comprises a contactless payment smart card 500 for use in a transit system. Figure 5 shows the reverse face 502 of the smart card 500. The smart card includes a base 504, which may be a plastic substrate. In other portable consumer devices, the base may comprise a structure such as a housing or internal circuit board, if the portable consumer device is a wireless phone or personal digital assistant (PDA) or keychain device. The card 500 includes a computer readable medium 506 comprising an interface for communication with the offline reader of

the associated transit processing system. The computer readable medium 506 can comprise a processor or logic chip with memory 506(a) and an antenna element 506(b). The antenna element is generally provided in the form of a coil and may be embedded within the base 504. The antenna element 506(b) may be powered by an internal or external source to allow for the contactless transmission of data to a card reader. The memory 506(a) stores the supplemental verification value described herein and can also be used to store Track 1 and Track 2 data, and the issuer verification value associated with conventional payment systems. In Figure 5, the memory 506(a) and antenna 506(b) are both embedded within the base 504 and therefore are illustrated in dotted line.

[0052] If desired, the reverse face 502 of the card 500 can include magnetic media or material 510 to store data for processing with a contact-type (online) reader of a payment system. Beneath the optional magnetic media 510 on the reverse face 502 is a signature block 512 on which the cardholder signature is written, and printed on the signature block is a four-digit card number value (shown as "9012" in Figure 5) and another three-digit CVV value 514 for typical online financial transaction processing.

[0053] Figure 6 is a representation of the Track 1 and Track 2 data of the contactless payment smart card illustrated in Figure 5. Those skilled in the art will be aware of Track 1 and Track 2 data formats in accordance with the well-known magnetic stripe data (MSD) configuration. Such data may be stored in the previously described memory 506(a) of the offline system interface 506. The data can be placed on the card in accordance with financial transaction processing of the ISO 7813 standard. The Track 1 data 602 includes data fields for the Primary Account Number (PAN), comprising a maximum of nineteen digits. The Track 1 data 602 also includes a name data field of twenty-six characters, an additional data field of seven digits, and a discretionary data field of eight digits. The Track 2 data 604 includes a 19-digit PAN field, an additional data field of seven digits, and a discretionary data field of eight digits. In conventional card construction in accordance with ISO 7813, the CCV data is stored in the additional data fields. For the contactless payment card of Figure 5 constructed in accordance with the invention, the supplemental verification value can be stored in one of the additional data fields.

[0054] Embodiments of the invention have a number of advantages. For example, in the context of a contactless payment card as described herein, offline processing can be provided without the need for configuring a second application (e.g., a transit application)

on the card in addition to a conventional payment application. In this way, the potential for counterfeiting cards is removed due to the inclusion of card authentication capability with the supplemental card verification value. There is also no need for the issuer to manage a second offline application on the card, thus saving space on the card. That is, a

5 supplementary application can be configured with the primary (e.g. retail) application data without need for a separate application. For example, if the card is used by a transit agency, the transit agency may utilize the same payment application configuration as all other merchants capable of processing contactless payments. There is no need for preregistration of the card at each transit location. Any encryption algorithms and keys or the like
10 necessary for offline processing will have been provided to the appropriate readers. This allows any transit system user to conduct transactions at any time using standard magnetic stripe type data. In addition, common key sets for the supplemental card verification value can be used and distributed to all issuers for personalization of the card and to all agencies for such validation. Moreover, there is no need for issuer/agency pre-agreement.

15 Standardized MSD track data can be used for both offline and online transactions.

[0055] It should be understood that certain elements of the present invention as described above can be implemented in the form of control logic using computer software in a modular or integrated manner. Based on the disclosure and teachings provided herein, a person of ordinary skill in the art will know and appreciate other ways and/or methods to
20 implement the present invention using hardware and a combination of hardware and software.

[0056] Any of the software components or functions described in this application, may be implemented as software code to be executed by a processor using any suitable computer language such as, for example, Java, C++ or Perl using, for example, conventional or
25 object-oriented techniques. The software code may be stored as a series of instructions, or commands on a computer readable medium, such as a random access memory (RAM), a read only memory (ROM), a magnetic medium such as a hard-drive or a floppy disk, or an optical medium such as a CD-ROM. Any such computer readable medium may reside on or within a single computational apparatus, and may be present on or within different
30 computational apparatuses within a system or network.

[0057] While certain exemplary embodiments have been described in detail and shown in the accompanying drawings, it is to be understood that such embodiments are merely

illustrative of and not intended to be restrictive of the broad invention, and that this invention is not to be limited to the specific arrangements and constructions shown and described, since various other modifications may occur to those with ordinary skill in the art.

- 5 **[0058]** As used herein, the use of "a", "an" or "the" is intended to mean "at least one", unless specifically indicated to the contrary.

WHAT IS CLAIMED IS:

1. A method of processing a transaction, the processing method comprising:

receiving data from a portable consumer device at a reader, wherein the portable consumer device stores an issuer verification value associated with an issuer and a supplemental verification value, and wherein the supplemental verification value is verified using an offline processing system that is not in communication with the issuer;

processing the supplemental verification value at the reader; and
authorizing the transaction if the processed supplemental verification value indicates that the portable consumer device is authenticated.

2. The method as defined in claim 1, wherein authorizing the transaction comprises permitting a user of the portable consumer device to enter a facility if the transaction is authorized.

3. The method as defined in claim 2, wherein the reader comprises a transit system reader.

4. The method as defined in claim 1, wherein processing the supplemental verification value comprises identifying an appropriate key and algorithm, and calculating a value corresponding to the portable consumer device and comparing the calculated value to the supplemental verification value received from the portable consumer device.

5. The method as defined in claim 4, wherein the supplemental verification value comprises a transit verification value.

6. The method as defined in claim 4, wherein the supplemental verification value is dynamically changed on the portable consumer device after issuance of the portable consumer device.

7. The method as defined in claim 4, wherein the supplemental verification value is static on the portable consumer device.

8. The method as defined in claim 1, wherein the supplemental verification value is stored in a supplemental data field of the portable consumer device.

9. The method as defined in claim 8, wherein the supplemental verification value is stored in track data of the portable consumer device in accordance with a magnetic stripe data (MSD) configuration.

10. The method as defined in claim 8, wherein the supplemental verification value is stored outside of track data of the portable consumer device, wherein the track data is defined in accordance with a magnetic stripe data (MSD) configuration.

11. The method as defined in claim 8, wherein the supplemental verification value is partially stored in track data of the portable consumer device in accordance with a magnetic stripe data (MSD) configuration and partially outside of the track data of the portable consumer device.

12. The method as defined in claim 1, wherein the portable consumer device comprises a contactless payment card.

13. The method as defined in claim 12, wherein the portable consumer device comprises a consumer electronic device.

14. The method as defined in claim 13, wherein the consumer electronic device comprises a wireless telephone.

15. The method as defined in claim 1, wherein the supplemental verification value is stored in a data track that is compatible with a payment processing system that processes data in accordance with a magnetic stripe data (MSD) configuration.

16. The method as defined in claim 1, further including:
generating a key and algorithm provided to the issuer and to the reader, wherein the reader processes the supplemental verification value using the key and algorithm.

17. A method of providing a portable consumer device, the method comprising:
receiving a supplemental verification value associated with an offline processing system; and

storing the supplemental verification value and an issuer verification value in the portable consumer device, such that data from the portable consumer device concerning a transaction can be received at a reader, wherein the issuer verification value is associated with an issuer, and wherein the supplemental verification value can be verified using an
5 offline processing system that is not in communication with the issuer such that the supplemental verification value can be processed at the reader and the transaction can be authorized if the processed supplemental verification value indicates that the portable consumer device is authenticated.

18. The method of claim 17, wherein the supplemental verification value
10 is a transit verification value that is used to authenticate the portable consumer device to gain access to a transit system.

19. The method of claim 17, wherein the received supplemental verification value comprises data created in accordance with a cryptography system.

20. The method of claim 19, wherein the supplemental verification value
15 and the issuer verification value are stored in a supplemental data field in a computer readable medium of the portable consumer device.

21. The method of claim 20, wherein the supplemental verification value is stored in track data of the portable consumer device in accordance with a magnetic stripe data (MSD) configuration.

22. The method of claim 20, wherein the supplemental verification value
20 is stored outside of track data of the portable consumer device, wherein the track data is defined in accordance with a magnetic stripe data (MSD) configuration.

23. The method of claim 20, wherein the supplemental verification value is partially stored in track data of the portable consumer device in accordance with a
25 magnetic stripe data (MSD) configuration and partially outside of the track data of the portable consumer device.

24. The method of claim 17, wherein the portable consumer device is a contactless portable consumer device.

25. The method of claim 17, wherein the portable consumer device is in the form of a card.

26. A portable consumer device comprising:
a base; and

5 a computer readable medium on the base, wherein the computer readable medium stores code for an issuer verification value and a supplemental verification value, wherein the issuer verification value is used by an issuer to verify that the portable consumer device is authentic in an online transaction and wherein the supplemental verification value is used to verify that the portable consumer device is authentic in an
10 offline transaction, such that data from the portable consumer device concerning a transaction can be received at a reader, wherein the issuer verification value is associated with an issuer, and wherein the supplemental verification value can be verified using an offline processing system that is not in communication with the issuer such that the supplemental verification value can be processed at the reader and the transaction can be
15 authorized if the processed supplemental verification value indicates that the portable consumer device is authenticated.

27. The portable consumer device as defined in claim 26, wherein the portable consumer device is a card.

28. The portable consumer device as defined in claim 27, wherein the
20 supplemental verification value is a transit verification value.

29. The portable consumer device as defined in claim 28, wherein the issuer verification value is stored in primary data of the portable consumer device and the transit verification value is stored in supplemental data of the portable consumer device.

30. The portable consumer device as defined in claim 29, wherein the
25 supplemental verification value is stored in track data of the portable consumer device in accordance with a magnetic stripe data (MSD) configuration.

31. The portable consumer device as defined in claim 29, wherein the supplemental verification value is stored outside of track data of the portable consumer

device, wherein the track data is defined in accordance with a magnetic stripe data (MSD) configuration.

32. The portable consumer device as defined in claim 29, wherein the supplemental verification value is partially stored in track data of the portable consumer device in accordance with a magnetic stripe data (MSD) configuration and partially outside of the track data of the portable consumer device.

33. The portable consumer device as defined in claim 28, wherein the supplemental verification value is stored in a data track that is compatible with a payment processing system that processes data in accordance with a magnetic stripe data (MSD) configuration.

34. The portable consumer device as defined in claim 26, wherein the portable consumer device is a contactless device.

35. The portable consumer device as defined in claim 26, wherein either the issuer verification value or the supplemental verification value can be dynamically changed in the portable consumer device.

36. The portable consumer device as defined in claim 26, wherein the issuer verification value and the supplemental verification value are statically stored in the portable consumer device.

37. The portable consumer device as defined in claim 26, wherein the portable consumer device comprises a wireless telephone.

38. A reader configured to receive data from a portable consumer device, wherein the portable consumer device stores an issuer verification value associated with an issuer and a supplemental verification value, and wherein the supplemental verification value is verified using an offline processing system that processes the supplemental verification value at the reader, and authorizes the transaction if the processed supplemental verification value indicates that the portable consumer device is authenticated.

39. The reader as defined in claim 38, wherein the reader is further configured to process the supplemental verification value by calculating a value using a predetermined key and algorithm, and comparing the calculated value to the supplemental

verification value read from the portable consumer device and thereby authenticate the portable consumer device.

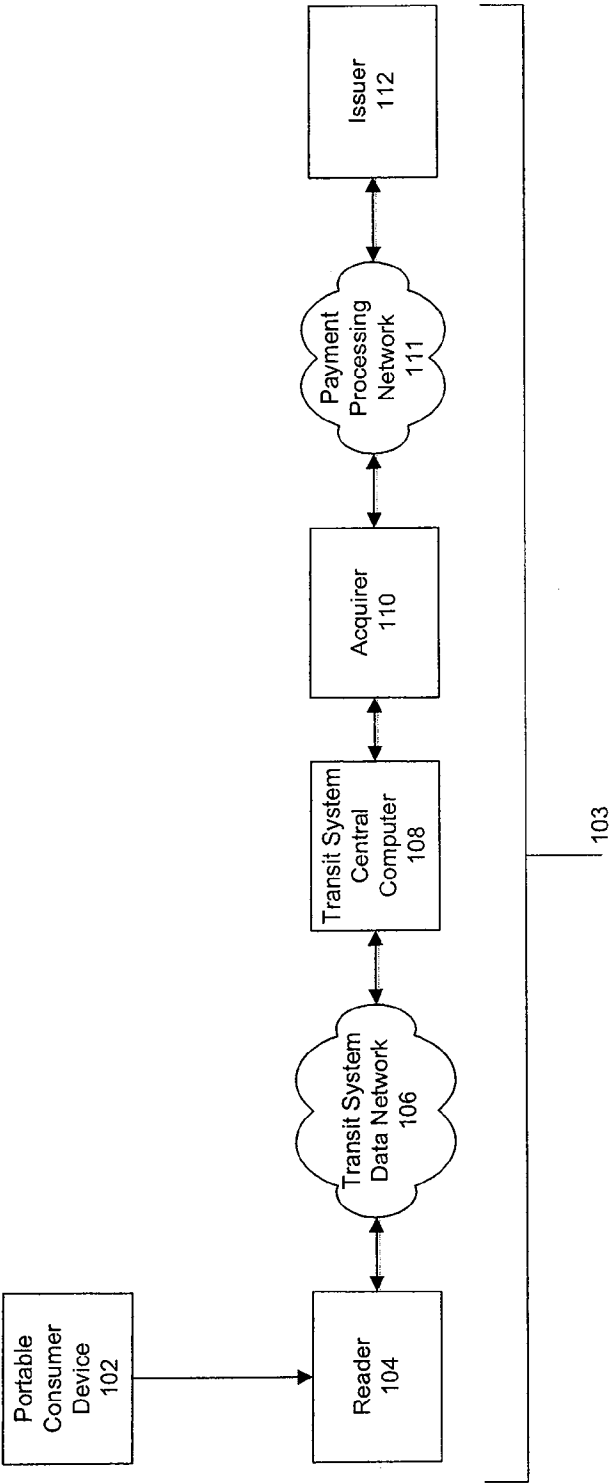


FIG. 1

2/5

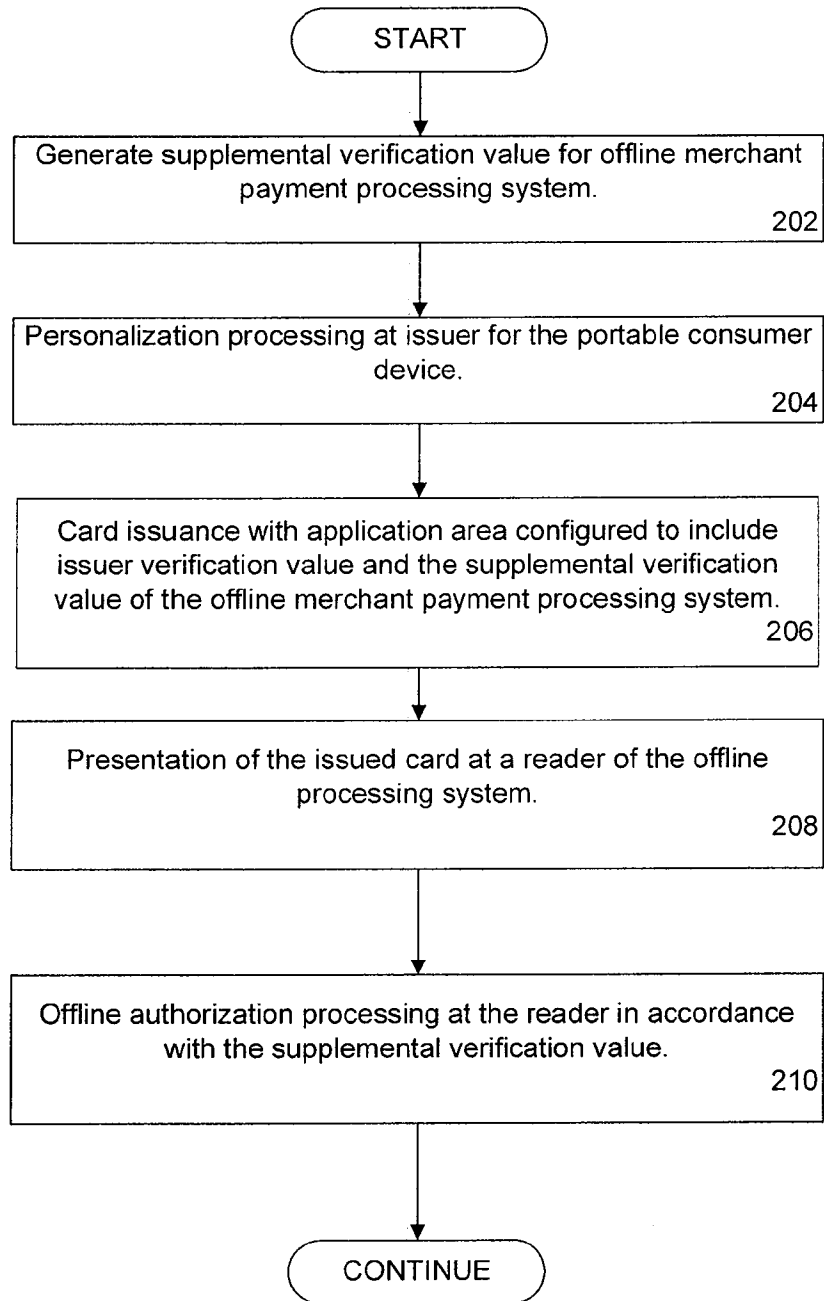


FIG. 2

3/5

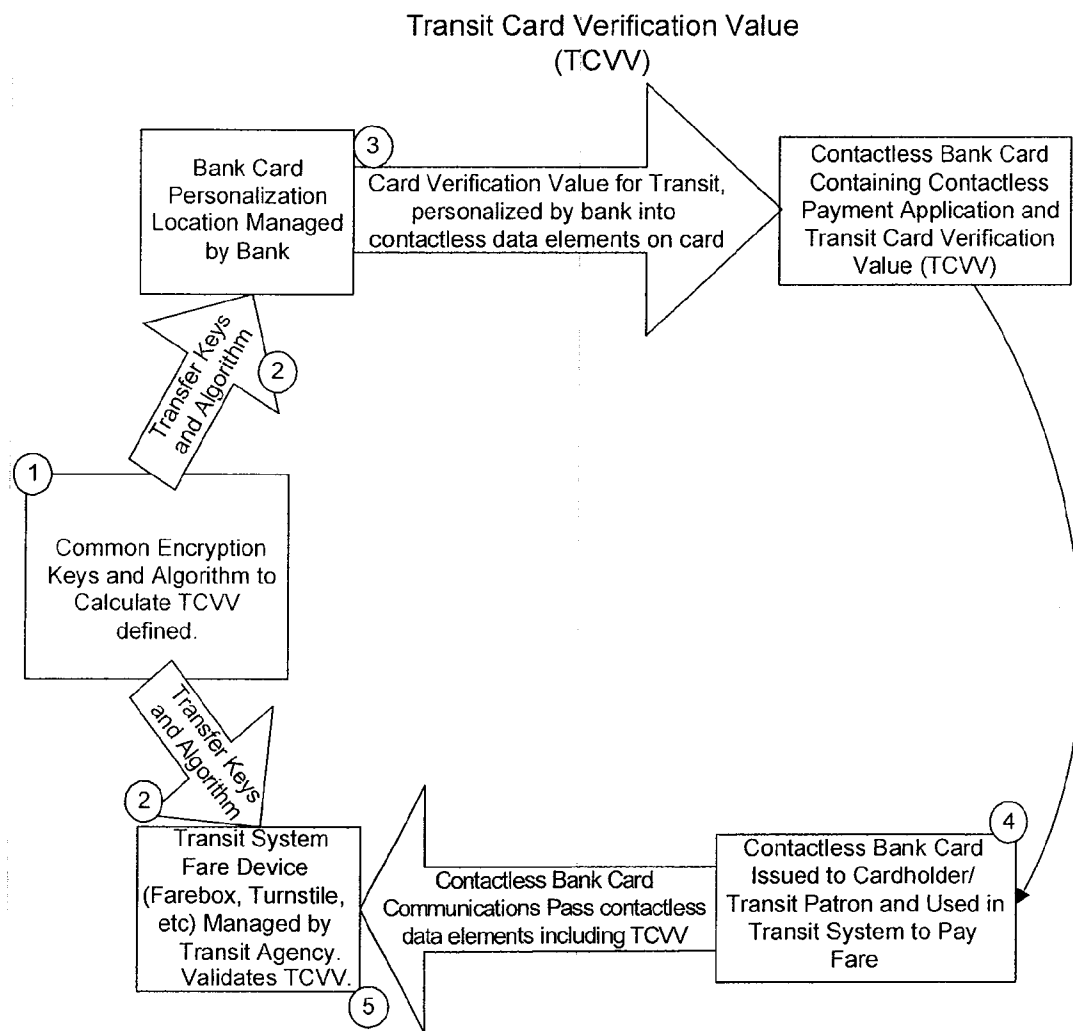


FIG. 3

4/5

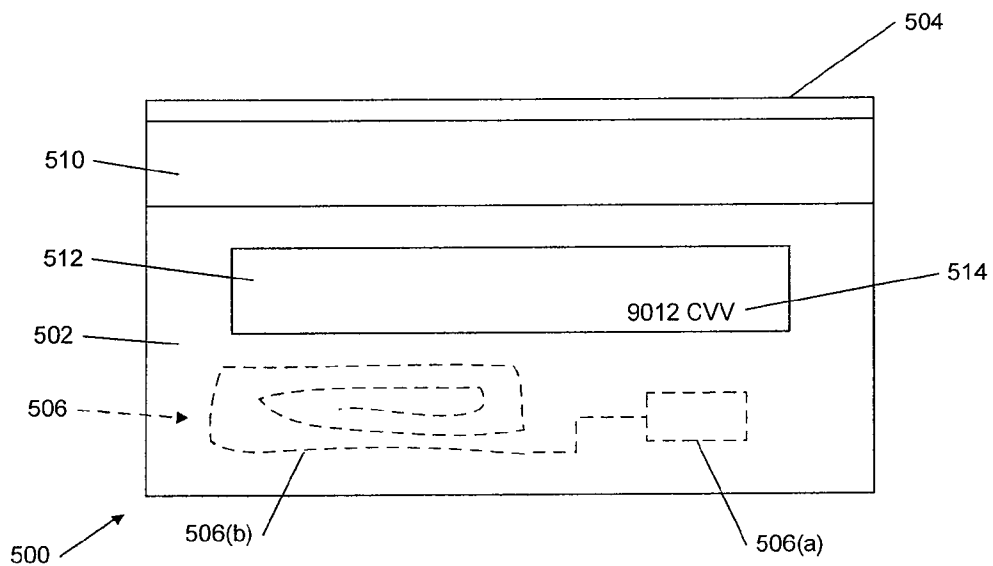
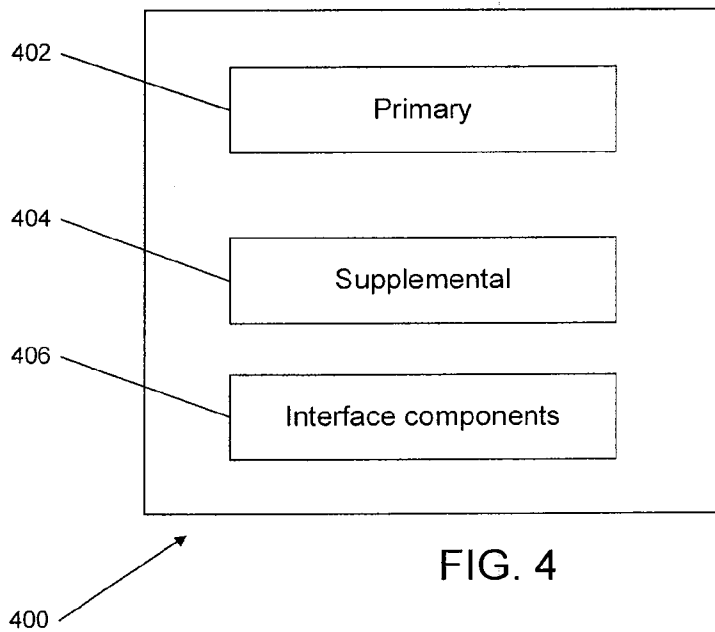
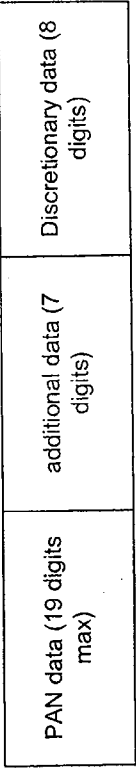


FIG. 5



602



604

FIG. 6