DATA PROTECTION WITH TRANSLATION

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] The present application is related to U.S. Provisional Application No. 61/583,550, filed on January 5, 2012 (Attorney Docket No.: 79900-819288), the entire contents of which are herein incorporated by reference for all purposes. The present application is also related to U.S. Provisional Application No. 61/607,546, filed on March 6, 2012 (Attorney Docket No.: 79900-829470), the entire contents of which are herein incorporated by reference for all purposes. The present application is further related to U.S. Provisional Application No. 61/704,428, filed on September 21, 2012 (Attorney Docket No.: 79900-851259), the entire contents of which are herein incorporated by reference for all purposes.

BACKGROUND OF THE INVENTION

[0002] Financial account data can be protected from unauthorized access through measures such as encryption of data within devices having hardware-based security controls. However, existing security measures, such as encrypting a personal identification number (PIN), may leave sensitive data, such as a primary account number (PAN) exposed. Existing solutions for protecting sensitive data may require application of key management schemes that differ from those used to encrypt PIN data, increasing the burden to merchants of providing security for financial data.

[0003] Merchants may protect financial account data by routing all transactions to a single destination for payment processing. However, when routing an authorization request for a transaction, a merchant may be able to select a payment processing network among multiple available payment processing networks. It may be necessary for the merchant to provide for decryption of information in the authorization request message and re-encryption of information based on the routing destination of the authorization request message. Some payment processing networks may lack an encryption solution for sensitive data. A merchant may wish to utilize the encryption measures provided by a first payment processing network while continuing to have the ability to route authorization requests to alternative payment processing networks.

[0004] Embodiments described herein solve these and other problems.

BRIEF SUMMARY OF THE INVENTION

[0005] Techniques are provided for protecting sensitive data when an authorization request for a transaction is routed in an environment comprising a plurality of payment processing network options.

[0006] In one embodiment, a method is described. The method includes encrypting a personal identification number (PIN) by an access device. The PIN encryption uses a first encryption key variant based on an initial key. The access device encrypts sensitive data using a second encryption key variant based on the initial key. An authorization request message including the encrypted PIN and encrypted sensitive data are transmitted to a host server.

[0007] In another embodiment, a method includes receiving an authorization request message at a host server. A secure module communicatively connected to the host server decrypts the encrypted sensitive data. The secure module re-encrypts the decrypted sensitive data with a first sensitive data zone encryption key associated with the first payment processing network. A first translated authorization request message including the re-encrypted sensitive data is transmitted by the host server to the first payment processing network. In a further embodiment, the authorization request message received at the host server includes a PIN. The secure module decrypts the encrypted PIN and re-encrypts the decrypted PIN with a first PIN zone encryption key associated with the first payment processing network. The first translated authorization request message includes the re-encrypted PIN. In an additional embodiment, the secure module is configured to transmit a second translated authorization request message to a second payment processing network. A second PIN zone encryption key is used for re-encryption of a PIN for the second translated authorization request message and a second sensitive data zone encryption key is used for re-encryption of sensitive data for the second authorization request message.

[0008] Another embodiment of the technology is directed to a system. The system includes a processor and a computer readable medium coupled to the processor. The

computer readable medium comprises code executable by the processor for implementing a method comprising encrypting a personal identification number (PIN) by an access device. The PIN encryption uses a first encryption key variant based on an initial key. The access device encrypts sensitive data using a second encryption key variant based on the initial key. An authorization request message including the encrypted PIN and encrypted sensitive data are transmitted to a host server.

[0009] A further embodiment of the technology is directed to a system. The system includes a processor and a computer readable medium coupled to the processor. The computer readable medium comprises code executable by the processor for implementing a method comprising receiving an authorization request message at a host server. The authorization request message includes encrypted sensitive data. A secure module communicatively connected to the host server decrypts the encrypted sensitive data. The secure module re-encrypts the decrypted sensitive data with a first sensitive data zone encryption key associated with the first payment processing network. A first translated authorization request message including the re-encrypted sensitive data is transmitted by the host server to the first payment processing network.

[0010] In a further embodiment, a method includes receiving data associated with a personal account identifier (PAI). An access device can encrypt the PAI. The encrypted PAI can have the same format as the PAI. The encrypted PAI is written to a field of an authorization request message. The field of the authorization request message is a field that is designated to receive a PAI. An authorization request message data element is used as a signal to identify the presence of the encrypted PAI in the authorization request message. The access device transmits the authorization request message.

[0011] These and other embodiments are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0012] FIG. 1 shows an exemplary system in which embodiments of the technology can be implemented.

[0013] FIG. 2 is an illustrative flowchart for encryption of PIN and sensitive data at the access device and merchant host.

[0014] FIG. 3 is an illustrative flowchart for translation of sensitive data at the host.

[0015] FIG. 4 is an illustrative flowchart for translation of PIN and sensitive data at the host.

[0016] FIG. 5 is a table showing an illustrative specification for the structure and content of track one of a payment device.

[0017] FIG. 6 is a table showing an illustrative specification for the structure and content of track two of a payment device.

[0018] FIG. 7 is a flow chart illustrating an implementation of format preserving encryption according to an embodiment.

[0019] FIG. 8 is a flow chart illustrating interpretation of data to determine whether format preserving encryption has been applied.

[0020] FIG. 9 depicts an illustrative high level block diagram of a computer system.

DETAILED DESCRIPTION OF THE INVENTION

[0021] Embodiments disclosed herein are directed to techniques for protecting financial data in an authorization request message. Terms used to describe embodiments herein can be understood with reference to the descriptions provided below.

[0022] An "authorization request message" can be a request to authorize a transaction. The authorization request message can be sent to an issuer of a payment account to request authorization of a transaction performed with the payment account. A merchant may generate the authorization request message. The authorization request message may be transmitted to the issuer via an acquirer.

[0023] The authorization request message may have a defined format to facilitate requests and responses between points in a financial network. For example, an authorization request message may be a standardized interchange message such as a

message that complies with International Organization for Standardisation (ISO) 8583, which is a standard for systems that exchange electronic transactions. An ISO 8583 message can include a message type indicator, one or more bitmaps indicating which data elements are present in the message, and data elements of the message. The data included in the authorization request message may include data obtained from a payment device as well as other data related to the transaction, the payment account holder, and the merchant. For example, the authorization request message can include a personal identification number (PIN), and sensitive data such as a primary account number (PAN), cardholder name, and discretionary data. Additionally, the authorization request message can include payment device expiration date, currency code, transaction amount, a merchant transaction stamp, acceptor city, acceptor state/country, routing transit number, terminal identification, network identification, etc. An authorization request message may be protected using encryption in order to prevent data from being compromised.

[0024] The authorization request message may include a payment account identifier. The payment account identifier may be associated with a portable consumer device, such as a credit card or debit card. For example, a payment account identifier may be a primary account number (PAN). The PAN may be a unique payment card number, such as a credit card account number associated with a credit card or a debit account number associated with a debit account. The PAN may identify the issuer as well as the cardholder account. Where the term PAN is employed herein, it will be understood that any payment account identifier could be used.

[0025] A personal identification number (PIN) can be a numeric password shared between a user and a system and used to authenticate the user to the system. A PIN block can be an encrypted block of data used to encapsulate a PIN. The PIN block may be composed of the PIN, the PIN length, and a subset of the PAN.

[0026] Issuer discretionary data (IDD), also referred to as "discretionary data," can be data residing in Track 1 and/or Track 2 of a magnetic strip or a chip of a payment device or otherwise associated with a payment account. The IDD may be variable in length and may contain customer and/or card verification data such as a PIN offset value, PIN verification value (PVV), card verification value (CVV), etc. The IDD may also include

other data defined by card brands and/or issuers, such as information used in a loyalty program, fleet data, etc.

[0027] An "acquirer" is typically a business entity (e.g., a commercial bank) that has a business relationship with a particular merchant. For example, the acquirer may deposit funds into a merchant bank account and recoup those funds from issuers.

[0028] An "issuer" is typically a business entity (e.g., a bank or credit union) which issues a payment device to an account owner and provides administrative and management functions for the payment account. Some entities may perform both issuer and acquirer functions. A payment account may be any account usable in a transaction, such as a credit, debit or prepaid account.

[0029] A "payment device" may refer to a device used to initiate a transaction, such as a portable consumer device or a portable communication device. The payment device may interface with an access device such as a point of sale device to initiate the transaction. Typically, a portable consumer device is hand-held and compact so that it can fit into a consumer's wallet or pocket (e.g., pocket sized). Specific examples of portable consumer devices include payment cards such as smartcards, debit devices (e.g., a debit card), credit devices (e.g., a credit card), or stored value devices (e.g., a stored value card or "prepaid" card). A portable communication device, also referred to as a "mobile device," may be, for example, a cellular or wireless telephone (e.g., a smartphone), personal digital assistant (PDA), portable computer (e.g., tablet or laptop computer), pager, or other portable device carried by the payment account holder.

[0030] An "access device" may refer to a device that receives information from a payment device to initiate a transaction. For example, an access device may be a point of sale device configured to read account data encoded in a magnetic stripe or chip of a card-format portable consumer device. Other examples of access devices include cellular phones, PDAs, personal computers, server computers, tablets, handheld specialized readers, set-top boxes, electronic cash registers, automated teller machines (ATMs), virtual cash registers, kiosks, security systems, access systems, and the like. Access devices may use means such as radio frequency (RF) and magnetic stripe readers to interact with a payment device. The access device may be a device located at a merchant's physical location or may be a virtual point of sale such as a web-site

that is part of an eCommerce (electronic commerce) transaction. In an eCommerce transaction, the account owner may enter payment account data into a portable communication device, personal computer, or other device capable of communicating with a merchant computer. In other card not present transactions, such as mail-order or telephone-order transactions, information may be entered into a merchant computer serving as an access device. In a further example, communication may occur between a contactless element of a portable communication device and an access device, such as a merchant device reader or point of sale terminal, by using a wireless communications mechanism, such as near field communications (NFC), RF, infra-red, optical communications, etc.

[0031] A "payment processing network" may include a system that receives an authorization request message. The payment processing network may obtain information from the authorization request message to use in determining whether to approve a transaction associated with the authorization request message. The payment processing network may send an authorization response message to the merchant indicating whether a transaction is approved. In some embodiments, the payment processing network may perform a settlement process, which can involve posting the transactions to the accounts associated with the payment devices used for the transactions and calculating the net debit or credit position of each user of the payment devices. A payment processing network may be operated by an acquirer and/or an issuer.

[0032] A "host" may be one or more systems, such as a server, responsible for performing merchant transaction processing, routing decision and/or capture. The host may be resident at a merchant, gateway, processor or other entity. In some embodiments, a host may be associated with a merchant direct exchange (MDEX), value added reseller (VAR), or other connectivity model. Where the term "merchant host server" is used herein, it will be recognized that any server, such as a payment processor server, could be used.

[0033] A "tamper-resistant security module" (TRSM) is a device that incorporates physical protections to prevent compromise of cryptographic security parameters contained by the device. TRSMs are available with varying levels of protection. A

TRSM that is tamper-resistant may employ physical measures such as hardened casing to make intrusion into the device difficult. A tamper-evident TRSM may have hardware features to make intrusion attempts evident to subsequent viewers, such as a seal that would be broken during intrusion into the device. A tamper-responsive TRSM may be configured to detect an intrusion attempt and destroy sensitive information, such as cryptographic security parameters, should an intrusion attempt occur.

[0034] A "hardware security module" (HSM) is a TRSM with a secure cryptoprocessor that can manage digital keys, accelerate cryptoprocesses and/or provide strong authentication for accessing critical keys for server applications. An HSM may provide both logical and physical protection of sensitive information from non-authorized access. The HSM may be a physical device in the form of a plug-in card or external security device. The HSM may be communicatively coupled to a host.

[0035] Payment card industry data security standards (PCI DSS) are a set of requirements applicable to entities involved with transaction processing. The purpose of the requirements is to maintain the security of financial data.

[0036] Derived Unique Key Per Transaction (DUKPT) is a key management scheme that can derive a unique transaction key for each transaction. DUKPT uses a base derivation key (BDK) that is typically known only to the party that initializes a TRSM and recipient of a message encrypted by the TRSM. The TRSM is typically injected with an initial key that is derived from the BDK. A transaction key may be derived from the initial key. If a derived key is compromised, future and past transaction data remain protected because the next or prior keys cannot be easily determined from the derived key. DUKPT can be used for the encryption of data associated with electronic commerce transactions, such as a PIN and/or sensitive data.

[0037] For example, a PIN pad may include a TRSM injected with a unique initial key and a key serial number. The PIN pad may generate a unique key for each transaction. An authorization request message generated by the PIN pad may include an encrypted PIN block and the key serial number. The authorization request message may be transmitted from the PIN pad to a merchant host server having its own TRSM. The merchant host server TRSM can use a key serial number (KSN) to retrieve the base

derivation key (BDK) used in the generation of the unique initial PIN pad key. The TRSM can use the BDK and the KSN to decrypt the encrypted data.

[0038] Triple Data Encryption Algorithm (TDEA), also referred to as "Triple Data Encryption Standard", "3DES," "Triple DES" and "TDES," is a block cipher that applies the Data Encryption Standard (DES) cipher algorithm three times to each block of data being encrypted.

[0039] A "Zone Encryption Key" (ZEK) can indicate one or more keys used to encrypt data between two specific points (e.g., between a host and a payment processing network). Separate ZEKs may be used for PIN and for sensitive data. In a preferred embodiment, ZEKs are used only for sensitive data encryption between parties, and is preferably not the same as PIN, MAC or other specific encryption keys

[0040] A "server" can include one or more computers. Multiple computers of a server may be communicatively coupled via network connections, such as wired, wireless, and/or internet network connections. One or more of the computers of a server may store databases.

ENCRYPTION AND ZONE TRANSLATION OF PIN AND SENSITIVE DATA

[0041] When a payment device is used for a transaction, an authorization request message may be generated for the transaction. The authorization request message may include a personal identification number (PIN) and sensitive data such as a primary account number (PAN), cardholder name, cardholder address, issuer discretionary data, or other sensitive data. Sensitive data may be data that is stored with a payment device, such as in the magnetic stripe or in a chip of the payment device. Alternatively, storage data may be data provided by a user to an access device, such as cardholder address information provided by a user in the course of an e-commerce or other card not present transaction. The PIN and sensitive data may be encrypted by an access device that receives information from the payment device. The PIN and sensitive data may be encrypted using encryption key variants based on an initial key injected into the access device.

[0042] FIG. 1 shows an exemplary system 100 in which embodiments of the technology can be implemented. System 100 includes one or more server computers,

data processing subsystems and networks that can be used to initiate an authorization request message for a transaction and route the authorization request message to an entity capable of approving the transaction. Where only one of each component is shown, it is understood that embodiments of the technology may include more than one of each component. In addition, some embodiments of the technology may include fewer than all of the components shown in FIG. 1. Also, the components in FIG. 1 may communicate via any suitable communication medium (including the internet), using any suitable communication protocol.

[0043] In a typical transaction, a payment device 102 interfaces with an access device 104 to initiate a transaction. Access device 104 may include access device tamper resistant security module (TRSM) 106. Access device TRSM 106 may be physically and/or communicatively coupled to (or may be an integral component of) access device 104. Access information can receive information associated with payment device 102, including sensitive data, when payment device 102 interfaces with access device 104. In some embodiments, access device 104 receives sensitive data and/or a PIN from a device storing account information, such as a portable communication device.

[0044] In an illustrative example, payment device 102 may be a credit card and access device 104 may be a PIN pad housed in a TRSM. The PIN pad may have a user interface for receiving numerical input indicating PIN passwords and a magnetic stripe reader for obtaining track data from the magnetic stripe of a payment device.

[0045] In other embodiments, payment device information may be user input that is received by access device 104. PIN data may be received from payment device 102 or from user input received by access device 106.

[0046] When access device 104 receives data such as PIN and payment device information, TRSM 106 may encrypt the data. In some cases, it may be necessary to obtain a PAN prior to encrypting the PIN. Sensitive data such as PAN, cardholder name, cardholder address, and discretionary data may be determined from the information received from payment device 102. The sensitive data may be parsed from track data obtained by access device 104 from payment device 102. In some embodiments, access device 106 encrypts the PIN by generating a PIN block based on the PIN, PIN length, and a subset of the PAN. Access device 104 may encrypt

sensitive data including one or more of PAN, cardholder name, cardholder address, discretionary data, and any other information to be treated as sensitive data.

[0047] Access device TRSM 106 may store an initial key used for encrypting data. For each transaction, one or more transaction keys may be derived from the initial key. It may be necessary for different transaction keys to be applied to PIN and sensitive data for compliance with regulations such as PCI DSS. The PIN may be encrypted using a first transaction key derived from the initial key and sensitive data may be encrypted using a second transaction key derived from the initial key. In this manner, both the PIN and the sensitive data can be encrypted using the same key management scheme (such as DUKPT) and the same encryption algorithm (such as TDEA).

[0048] An authorization request message including encrypted PIN data and encrypted sensitive data may be generated by access device 104 and transmitted to merchant host server 108. The authorization request message may include designated fields for various types of data. When encryption is applied to data in an authorization request message, the encryption may change parameters (such as data type, data length, etc.) of a field associated with the encrypted data. Due to the changed parameters, the encrypted data may be placed in a new field. For example, an authorization request message may include a field sized to accommodate a PAN. When the encryption is applied, the PAN and other sensitive data may be placed in one or more alternative fields of the authorization request message. A field may be added to an authorization request message to signal that the encrypted PAN is located in an encrypted PAN field. Sensitive data such as a PAN, a cardholder name, and discretionary data may be encrypted at access device 104 and placed in individual elements within a field of an authorization request message, such as field 53 of an ISO formatted authorization request message.

[0049] In some embodiments, format preserving encryption is applied to sensitive data in the authorization request message. For example, when format preserving encryption is used, a subset of the digits of the PAN may be replaced with encrypted values while particular digits of the PAN remain unchanged. In a preferred embodiment, the first six digits and the last four digits of the PAN remain unchanged and the middle digits are replaced with encrypted values. In this manner, the authorization request message can

be handled by payment processing networks that are not configured to handle authorization request messages having alternative fields for storing encrypted data. To signal the presence of encrypted data within the PAN field of the authorization request message, an altered expiration date may be included in the expiration date field of the authorization request message. For example, the authorization request message may contain an expiration date that is 40 years after the expiration date associated with the payment device used for a transaction.

[0050] Merchant host server 108 may include merchant host TRSM 110. Merchant host TRSM 110 may be communicatively and/or physically coupled to or an integral component of merchant host server 108. In some embodiments, merchant host TRSM 110 may be located remotely from the premises of merchant server 108. In order to route transactions to multiple payment processing networks, a merchant may need to have a merchant host TRSM 110 to translate encrypted data in the authorization request message. For example, it may be necessary to translate keys at a merchant host TRSM 110 for compliance with PCI DSS standards limiting the exposure of keys associated with access device TRSM 106. When merchant host server 108 is configured to route authorization request messages to multiple payment processing networks 112-116, merchant host server 108 may translate encrypted data into a Zone Encryption Key (ZEK) associated with a particular payment processing network. Merchant host server 108 may determine how to route an authorization request message based on information contained in the authorization request message. For example, the first six digits of a PAN field containing a PAN encrypted according to a format preserving encryption method may be used by merchant host server 108 to determine how to route the authorization request message.

[0051] Translation by merchant host TRSM 110 can include decryption of PIN and sensitive data in the authorization request message received from access device 104 and re-encryption of the PIN and sensitive data using one or more Zone Encryption Keys (ZEK). A ZEK may be associated with a particular payment processing network. The ZEK is typically a shared key between a payment processing network and merchant host server 108. It may be necessary to apply different ZEKs to PIN and to sensitive data, e.g., for compliance with PCI DSS. The translation may be performed by Merchant Host TRSM 110 such that decrypted PIN and sensitive data are never

exposed to merchant host server 108. Merchant host server 108 may transmit an authorization request message including the translated PIN and sensitive data to the one of payment processing networks 112-116 to which the authorization request message is to be routed.

[0052] In some embodiments, merchant host server 108 may route an authorization request message to a payment processing network that is not configured to handle encrypted data. In such embodiments, encrypted sensitive data may be decrypted and an authorization request message including the decrypted sensitive data may be transmitted from merchant host server 108 to the payment processing network.

[0053] The payment processing network that receives the authorization request message may decrypt the PAN or other sensitive data and may also verify the PIN. The payment processing network may determine whether the transaction is authorized. In some cases, the authorization request message can be transmitted to an issuer server which may determine whether the transaction is authorized. An authorization response message indicating whether the transaction was authorized may be routed back to merchant host server 108 from the issuer and/or payment processing network that received the authorization request message. The authorization response may be displayed by the access device 104, printed on a receipt, or otherwise conveyed to the payment account holder.

[0054] It will be understood that a server associated with a payment processing network or other entity and associated TRSM can be used in lieu of merchant host server 108 and merchant host TRSM 110.

[0055] A clearing and settlement process is typically conducted by each of the payment processing networks at a fixed time. The fixed time may vary from one network to another. A clearing process is a process of exchanging financial details between an acquirer and an issuer to facilitate posting to the payment account holder's account and reconciliation of the consumer's settlement position.

[0056] Within a TRSM, data may be encrypted and/or decrypted using DUKPT and TDES. It will be recognized that other key management systems (such as

master/sesion and fixed key) and/or other encryption algorithms (such as RSA, DEA, ECIES, AES, or other encryption algorithms) could be applied.

[0057] FIG. 2 is an illustrative flowchart for encryption of PIN and sensitive data at the access device and merchant host. At operation 202, the cardholder can present a payment device 102 at access device 104. At operation 204, access device 104 can read data from payment device 102, such as track data stored in the magnetic stripe of the payment device. The data read from payment device 102 can include sensitive data, such as a PAN, cardholder name, and discretionary data. At operation 206, access device 104 can receive a PIN, such as a PIN entered at a user interface of access device 104.

[0058] At operation 208, access device 104 can encrypt the PIN using a first key. The first key may be a first transaction specific key derived from a key injected into access device 104. At operation 210, access device 104 can encrypt sensitive data using a second key. Sensitive data may include one or more of a PAN, cardholder name, discretionary data, cardholder address, and any other sensitive data received by acess device 104. The second key may be a second transaction specific key derived from a key injected into access device 104. At operation 212, access device 104 can generate an authorization request message including the encrypted PIN and encrypted sensitive data and transmit the authorization request message to a host server, such as merchant host server 108.

[0059] In some embodiments, an host device may receive an authorization request message including encrypted sensitive data from an access device. The authorization request may or may not include an encrypted PIN. For example, an access device may receive sensitive data from a credit card or other payment device for a transaction that does not require a PIN number. In such embodiments, a host device may translate sensitive data.

[0060] FIG. 3 is an illustrative flowchart for translation of sensitive data at the host. At operation 302, a host such as merchant host server 108 receives an authorization request message including encrypted sensitive data from access device 104. The host may parse the sensitive data from the authorization request message. At operation 304, the host may decrypt sensitive data using information derived from a base

derivation key. To translate the sensitive data, the host may decrypt the sensitive data using the information derived from the base derivation key associated with access device 104, as indicated at operation 304, and re-encrypt the sensitive data using a zone encryption key, as indicated at operation 306. At operation 308, the host may transmit an authorization request message to the payment processing network.

[0061] In some embodiments, a host may receive an authorization request message including an encrypted PIN and encrypted sensitive data. The host may translate the PIN and the sensitive data.

[0062] FIG. 4 is an illustrative flowchart for translation of PIN and sensitive data at the host. At operation 402, a host such as merchant host server 108 receives an authorization request message including an encrypted PIN and encrypted sensitive data from access device 104. Decrypted sensitive data such as a decrypted PAN may be needed for decryption of the PIN. The host may parse the sensitive data from the authorization request message At operation 404, the host may decrypt sensitive data using information derived from a base derivation key. The host may parse the PIN from the authorization request message. At operation 406, the host may decrypt the PIN using the information derived from the base derivation key, and, in some cases, also using the decrypted PAN. To translate the PIN, the host may re-encrypt the PIN using a zone encryption key, as indicated at operation 408. In some embodiments, the PIN is re-encrypted using the zone encryption key and the decrypted PAN. To translate the sensitive data, the host may re-encrypt the sensitive data using a zone encryption key, as indicated at operation 410.

[0063] In some embodiments, separate zone encryption keys may be used to encrypt the PIN and the sensitive data. For example, a PIN-specific zone encryption key may be used or generated for use in encrypting PIN numbers, and a sensitive-data-specific zone encryption key may be used or generated for use in encrypting sensitive data. Furthermore, each payment processing network 112-116 may use one or more zone encryption keys that are specific to the particular payment processing network. Thus, a first PIN-specific zone encryption key and a first sensitive-data-specific zone encryption key can be used for translation when an authorization request message will be routed to a first payment processing network 112, and a second PIN-specific zone encryption key

and a second sensitive-data-specific zone encryption key can be used for translation when an authorization request message will be routed to a second payment processing network 114.

[0064] Merchant host server 108 may determine which payment processing network of payment processing networks 112-116 is to receive the authorization request message. At operation 412, the merchant host server 108 may transmit an authorization request message including the translated (re-encrypted) PIN and translated (re-encrypted) sensitive data to the determined payment processing network.

[0065] In some embodiments, merchant host server 108 includes "white list" support for allowing specific card ranges defined by the merchant or payment processing network to be excluded from protection. When sensitive data is encrypted at access device 104, a part of the sensitive data may be may be maintained in cleartext for use at access device 104. For example, some or all of the data in the discretionary data field or other field of the track data on the magnetic stripe of payment device 102 may remain unencrypted in the authorization request message. Merchants that use data in the discretionary data field for loyalty programs, fleet programs, or the like may require that this data remain unencrypted for data gathering or other purposes.

[0066] In some embodiments, a cardholder name and/or data in the discretionary data field may be made available to the access device prior to encryption. For example, if an application executed by the access device or another merchant device uses this sensitive data (e.g., displaying a cardholder name at a cash register communicatively connected to a PIN pad device), the sensitive data may be exposed to the merchant device prior to encryption.

[0067] As discussed above, a chip or magnetic stripe in a payment device may have one or more tracks (typically three tracks, referred to as "track one," "track two," and "track three") that hold data. The data may be formatted in accordance to a standardized structure. FIGS. 5 and 6 are tables showing illustrative specifications for payment device track data It will be recognized that track data having the structure described in FIGS. 5 and 6 may be stored in association with a payment account on a portable media device or other device used for ecommerce or other card not present transactions.

[0068] FIG. 5 is a table showing an illustrative specification for the structure and content of track one of a payment device. Track 1 is encoded with a 7-bit scheme that is based on ASCII. Track 1 fields can include a start sentinel (such as "%"), indicating the position at which the formatted track data begins.

[0069] A format code (such as "B," indicating a financial institution) is typically the next character in track 1.

[0070] The Primary Account Number (PAN) can be comprised of a six digit Issuer Identification Number (IIN), a variable length (maximum 12 digits) individual account number and a check digit. The end of the data associated with the PAN can be indicated with a separator character, such as a caret (^).

[0071] The name field may include a single alpha character (as surname) and the surname separator. The space character may be required to separate the logical elements of the name field other than the surname. The separator terminating the name field may be encoded following the last logical element of the name field. If only the surname is encoded, the Field Separator (FS), such as "^" can follow the surname. In some embodiments, the name field includes a surname, followed by a surname separator (e.g., the "/" character), followed by a first name or initial, followed by a space, followed by a middle name or initial. The name can additionally include a period after the middle name or initial, followed by a title. The name is typically ended with a separator (the character "^"). For example, the name John C. Smith may be encoded as "SMITH/JOHN C".

[0072] The expiration field of track one may have the format YYMM, where 'YY' represents the last two digits of the year and 'MM' is the numeric representation of the month.

[0073] The service code may be a numeric field with three sub-fields represented by individual digits. Typically, the service code is used to indicate the issuer's acceptance criteria for magnetic stripe transactions and whether a related integrated circuit supporting the equivalent application as identified by the magnetic stripe or embossing is present on the card. Each sub-field of the service code can be identified by its

position (position 1, 2 and 3) and can operate independently, allowing judgments on its separate functions.

[0074] Issuer discretionary data may follow the service code. The end of the track is indicated by an end sentinel, such as a question mark character ("?"). Following the end sentinel, a longitudinal redundancy check character (LRC) may be included.

[0075] FIG. 6 is a table showing an illustrative specification for the structure and content of track two of a payment device. The character codes in track two are based on a 5-bit scheme that is based on ASCII. Track two may contain similar fields to those contained in track one, as described above, but may lack a cardholder name field.

[0076] In some embodiments, PIN data may be stored on and read from track three of a payment device.

ENCRYPTION WITH OBFUSCATION

[0077] After encryption is performed on data fields associated with payment device 102, encrypted information may be stored in one or more alternate fields of the authorization request message and obfuscated data may be stored in the original fields of the authorization request message. For example, data may be read from the PAN, cardholder name, and discretionary data fields associated with payment device 102. Obfuscated data may be written to the fields of the authorization request message designated for the PAN, cardholder name, and discretionary data and encrypted versions of the PAN, cardholder name and discretionary data may be written to one or more alternate fields of the authorization request message.

[0078] In an illustrative example, for an authorization request message that complies with ISO standards, an alternate field such as ISO field 53 may be defined to receive encrypted data and associated encryption attributes. The new definition of ISO field 53 may conform to the "composite" field type as defined in the ISO standard. The new field 53 may receive encrypted PIN block data and encrypted sensitive data. When zone encryption is applied to an authorization request message, zone encryption may be applied to field 53.

[0079] When obfuscated data is written to a PAN field of an authorization request message, some digits of the PAN in the retained PAN field can be maintained and other

digits of the PAN can be obfuscated. For example, a subset of digits of the PAN, e.g. digits 7-12 (the "middle six" digits) of the PAN, can be obfuscated, while other digits, such as the first six and last four digits of the PAN, remain as plain text. Obfuscation may be performed, for example, by replacing digits 7-11 of the PAN with the number 9 and replacing digit 12 of the PAN with a number calculated to insure that the last digit of the PAN is a valid check digit. Because the remaining digits of the PAN, such as the first six digits and the final four digits, are not obfuscated, the remaining digits can be used for functions such as routing and receipt determination. In this manner, systems that are designed to handle data contained in the PAN field can function normally although the PAN is protected through obfuscation of the middle six digits. The encrypted PAN stored in an encrypted PAN field can be decrypted, allowing the decrypted (original) PAN to be written into the PAN field.

FORMAT PRESERVING ENCRYPTION

[0080] It may be desirable to encrypt data contained in the authorization request message without altering the format of the authorization request message. For example, some systems may not be designed to handle an authorization request message having an added encrypted PAN field. Format preserving encryption may be applied to sensitive data such as PAN, cardholder name and discretionary data from track 1 and track 2 of the track data associated with payment device 102.

[0081] A PAN may be encrypted such that the resulting encrypted PAN has the same size as the original PAN. In this manner, the encrypted PAN can be written to the original PAN field of the authorization request message, and no alternate field of the authorization request message is required to receive an encrypted PAN. Some digits of the PAN may remain unencrypted when format preserving encryption is applied to the PAN. For example, the first six and last four digits of the PAN may remain unencrypted to allow for routing and other functions dependent on data contained in these digits.

[0082] Format preserving encryption may function differently for PANs that contain valid check digits. An algorithm for determination of valid check digits may be as defined in ISO standards. The check digit, which is typically the final digit of the PAN, may be a digit computed from the other digits in the message that can be used to determine whether all digits of the PAN were correctly received. The check digit may be

used to detect transmission errors. In some embodiments, the last digit of digits 7-12 (the "middle six" digits) of the PAN is calculated such that the original last digit of the unencrypted PAN is still a valid check digit for the PAN encrypted with format preserving encryption. When a PAN does not contain a valid check digit, all middle digits may be encrypted with a format preserving encryption algorithm.

[0083] Sensitive data may be converted into the a base-10 alphabet prior to encryption. After the format preserving encryption algorithm has been applied, the resulting encrypted characters in base-10 alphabet form may be converted to the original code set and format of the original sensitive data. The converted encryption result may be used to replace the original fields for sensitive data such as PAN, cardholder name, discretionary data, etc. in the authorization request message.

[0084] Typically, it will not be apparent from the data in the fields to which format preserving encryption has been applied that the data has been encrypted. A signal may be used in an existing data field of the authorization request message to indicate that a field of an authorization request message contains encrypted data. To implement the signal, a field of the authorization request message that does not contain encrypted data can be overwritten with new contents that are a modified version of the original contents of the field. For example, an expiration date in an expiration date field of the authorization request message can be replaced with an altered expiration date. In one embodiment, the altered expiration date is obtained by adding a number to the expiration date or a portion of the expiration date. For example, a number such as 40 may be added to the year portion of the expiration date. If an expiration date field of an authorization request message contained an expiration date of "01/13," indicating an expiration date of January 2013, the number 40 can be added to year portion 13 and the resulting altered expiration date "01/53" can be written to the expiration date field. If a transaction takes place in 2013, a device reading the expiration date portion of the authorization request message may be able to determine that the expiration date is an altered expiration date because payment devices are typically issued with an expiration date that is under 20 years (e.g., 1-10 years) from the date the card issues. On this basis, it can be determined that an expiration date that is over twenty years past the present date is an altered expiration date.

[0085] In some embodiments, the last digit of the PAN may not contain a valid check digit. For example, the last digit of the PAN may not have a check digit as specified by ISO/IEC standard 7812-1. In cases where the last digit of the PAN is not a valid check digit, the number 20 may be added to the month of the expiration data before the altered expiration date is written to the expiration date field of the authorization request message.

[0086] In some embodiments, the expiration date field may be missing from the information received by access device 104. For example, a card read or key entry may have errors or otherwise lack the expiration date. The number 40 may be added to the month of the expiration date created in the format preserving encryption process before the altered expiration date is written to the expiration date field of the authorization request message.

[0087] Below, an exemplary algorithm for format preserving encryption is described. The format preserving encryption algorithm may operate as a stream cipher that is format preserving. For example, the format preserving encryption may be similar to the Counter Mode (CTR) from the National Institute Standards and Technology (NIST) standard SP800-38A, generalized to modulo-n addition instead of modulo-2 addition.

[0088] In the format preserving algorithm, A may be an alphabet with n different characters, where n is a natural number greater than 1. A^* may be denoted as the set of strings with elements from A, including the empty string. In this description it is assumed that the alphabet A is the set $\{0, \ldots, n\text{-}1\}$. If this is not the case, a translation is needed, based on the number of different characters in the alphabet A. The translation may happen prior to encryption, and again, after decryption, so that encryption and decryption will always work on alphabets of the form $\{0, \ldots, n\text{-}1\}$ for some positive integer n, greater than 1.

[0089] The format preserving encryption algorithm may use Counter (CTR) mode as defined in SP800-38A with a block cipher CIPH (AES or TDEA) with block size b bits, and encryption key K for CIPH, and a sequence of counter blocks (called counters in SP800-38A) $T_1, T_2, \ldots$, to produce a sequence of output blocks, one for each counter block. Each output block consists of k base-n digits, where k is a configurable

parameter which must be chosen from the interval $[1, \ldots, \lfloor \log_n 2^b \rfloor]$. For reasons explained below, each counter block is b-7 bits, rather than b bits as in SP800-38A. The mechanism for how to produce the output blocks is also described below.

[0090] To encipher a plaintext P of length L, with 1≤L, as many output blocks as necessary (but no more) are generated, so that the total number of base-n digits in the output blocks is at least L, that is, we calculate the unique integers p and r such that $\frac{L}{k} \leq p < \frac{L}{k} + 1$ and 0 ≤r<k, such that $L=pk-r$, and generate output blocks G1,..., Gp .

Then each plaintext base-n digit $P[i]$ is added, modulo-n, to the ith base-n digit from the concatenation of the output blocks, $G_1 \| G_2 \| \ldots \| G_p$, to form the ith digit of the ciphertext:

[0091] $$C[i] = \left(P[i] + (G_1 \| \ldots \| G_p)[i]\right) \bmod n.$$

[0092] Since k may not divide L, some digits of the last output block, Gp may be ignored. The last r base-n digits of G_r are not used.

[0093] To decipher a ciphertext C of length L, with 1≤L, as many output blocks as necessary (but no more) are generated, so that the total number of base-n digits in the output blocks exceed L, which is done in the same way as for encryption. Then from each ciphertext base-n digit $C[i]$ is subtracted, modulo-n, the ith base-n digit from the concatenation of the output blocks, $G_1 \| \ldots \| G_p$, to form the ith digit of the plaintext:

[0094] $$C[i] = \left(P[i] + (G_1 \| \ldots \| G_p)[i]\right) \bmod n.$$

[0095] For format preserving encryption, as for Counter mode itself, the sequence of counter blocks must have the property that each block in the sequence is different from every other block. This condition is not restricted to a single encryption: across all of the messages that are encrypted under a given key K, all counters must be distinct. SP800-38A describes methods for generating counters.

[0096] Given a block cipher CIPH with block length b, a key K for CIPH, a b-7 bit counter T, a natural number n>1, which is the base of the plaintext to be enciphered, and an integer k with $0 < k \leq \lfloor \log_n(2^b) \rfloor$, an output block consisting of k base-n digits is produced in the following way:

[0097] A 7-bit counter, S, is initialized to 0. Then CIPHK is applied to $S \| T$ to produce a block B of b bits. B is interpreted as an integer in the interval $\{0,\ldots,2^b-1\}$, and if $B < n^k \left\lfloor \frac{2^b}{n^k} \right\rfloor$, then it is accepted, otherwise S is incremented and CIPHK is applied again to $S \| T$, etc., until B is accepted or S equals 127. If $S = 127$, an error is raised, otherwise B is converted to base-n and is the k-digit base-n output block, possibly with leading zeros. Under the assumption that CIPHK is a pseudorandom permutation, the probability in each iteration that B is accepted is at least 0.5, and the probability that an error is raised is at most 2^{-128}. The pseudocode below describes this algorithm:

```
i = 0;
Input_Block = Si || T ;
max_B = (n^k)*((2^b) div (n^k));
B = CIPH(K, Input_Block);
while ( (AsInteger(B) ≥ max_B) AND (i < 127)) {
  i = i+1;
  Input_Block = Si || T ;
  B = CIPH(K, Input_Block);
};
if (i=127) return ERROR;
Output_Block = Convert(B, k, n);
return Output_Block;
```

[0098] Here it is assumed that S_0, S_1, ..., S_{127} enumerate the 128 different 7-bit combinations, that "AsInteger" takes a string of b bits $B[1]$, ..., $B[b]$ and converts it to the integer $\sum_{i=1}^{b}(B[i] \cdot 2^{b-i})$, and that "Convert" converts B to k base-n digits, with leading zeros if necessary:

```
Convert(B, k, n) {
        M = AsInteger(B);
        for (i=1; i≤k; i++){
                D[i] = M mod n;
                M = M div n;
        };
        return D;
}
```

[0099] The maximum value for L, that is, the bit length of the longest plaintext that can be enciphered is $2^{b/2}$.

[0100] The upper bound $n^k \left\lfloor \frac{2^b}{n^k} \right\rfloor$ for B interpreted as an integer is chosen as the largest possible whole multiple of n^k, that makes it possible to extract a k-digit base-n number uniformly from it, assuming the distribution of B is uniform.

[0101] FIG. 7 is a flow chart illustrating an implementation of format preserving encryption according to an embodiment. The operations described with reference to FIG. 7 may be performed, for example, by an access device or a host. At operation 702, a PAN is read. The PAN may be read by access device 104 from payment device 102. Alternatively, the PAN may be read from a PAN field of an authorization request message.

[0102] At operation 704, at least a part of the PAN is encrypted such that the length of the encrypted PAN is equal to the length of the original PAN. The PAN may be encrypted by access device 104 or merchant host server 108. At operation 706, the encrypted PAN may be written to the PAN field of the authorization request. At operation 708, the expiration date can be read from the expiration date field of the authorization request message (or from the payment device). At operation 710, an altered expiration date can be written to the authorization request message. An altered expiration date may be generated by, for example, adding a number to the year portion of the original expiration date. The number added to the original expiration date may be a number between 5-99, such as a number between 10 and 50, e.g., 40. It will be recognized that alternative algorithms, such as subtraction of a number from the original expiration date, may be used.

[0103] FIG. 8 is a flow chart illustrating interpretation of data to determine whether format preserving encryption has been applied. The operations described with reference to FIG. 8 may be performed, for example, by merchant host server 108, a payment processing network 112-116, an issuer, an acquirer, etc. At operation 800, an authorization request message is received. For example, the authorization request message may be received by merchant host server 108 or a payment processing

network. At decision diamond 802, it may be determined whether the year portion of an expiration date read from the expiration date field of an authorization request message is less than a particular number of years from the current date, e.g., 20 years from the current date. If the expiration year is less than 20 years from the current date, no signal for format preserving encryption is present in the authorization request message, as indicated at 804. If the expiration date is more than 20 years from the current date, unencrypted data of the PAN can be read from the PAN field, as indicated at operation 806. The unencrypted PAN data may be used for routing (e.g., by the merchant host server 108), fraud detection, authorization determination, or other purposes.

COMPUTER SYSTEM

[0104] FIG. 9 is an illustrative high level block diagram of a computer system that may be used to implement any of the entities or components described above (e.g., the access device, host, payment processing network, acquirer processor, etc.). The subsystems shown in FIG. 9 are interconnected via a system bus 902. Additional subsystems such as a printer 904, keyboard 906, fixed disk 908, and monitor 910, are coupled to display adapter 912. Peripherals and input/output (I/O) devices, which couple to I/O controller 914, can be connected to the computer system by any number of means known in the art, such as serial port 916. For example, serial port 916 or external interface 918 can be used to connect the computer apparatus to a wide area network such as the Internet, a mouse input device, or a scanner. The interconnection via system bus 902 allows the central processor 920 to communicate with each subsystem and to control the execution of instructions from system memory 922 or the fixed disk 908, as well as the exchange of information between subsystems. The system memory 922 and/or the fixed disk 908 may embody a computer readable medium.

[0105] As described, the inventive service may involve implementing one or more functions, processes, operations or method steps. In some embodiments, the functions, processes, operations or method steps may be implemented as a result of the execution of a set of instructions or software code by a suitably programmed computing device, microprocessor, data processor, or the like. The set of instructions or software code may be stored in a memory or other form of data storage element which is

accessed by the computing device, microprocessor, etc. In other embodiments, the functions, processes, operations or method steps may be implemented by firmware or a dedicated processor, integrated circuit, etc.

[0106] It should be understood that 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 implement the present invention using hardware and a combination of hardware and software.

[0107] 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 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 computational apparatuses within a system or network.

[0108] 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.

[0109] 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 comprising:

receiving, by an access device, a personal identification number (PIN) and sensitive data;

encrypting, by the access device, the PIN, wherein PIN encryption uses a first encryption key variant based on an initial key;

encrypting, by the access device, the sensitive data, wherein sensitive data encryption uses a second encryption key variant based on the initial key; and

transmitting, to a host server, an authorization request message including the encrypted PIN and encrypted sensitive data.

2. The method of claim 1, wherein the initial key is generated by a derived unique key per transaction (DUKPT) key management scheme.

3. The method of claim 1, wherein at least one of the PIN and the sensitive data are encrypted using Triple DES Encryption Algorithm (TDEA).

4. The method of claim 1, wherein the sensitive data includes at least one of a primary account number (PAN), a cardholder name, a cardholder address, and discretionary data.

5. The method of claim 1, wherein a subset of discretionary data remains unencrypted when discretionary data is included in encrypted sensitive data.

6. The method of claim 1, wherein an encrypted PAN is written to the PAN field of the authorization request message, wherein the encrypted PAN has the same format as the unencrypted PAN.

7. The method of claim 6, wherein a subset of digits of the unencrypted PAN remain unencrypted in the encrypted PAN.

8 . The method of claim 6, wherein an expiration date field of the authorization request message is overwritten with an altered expiration date to indicate that the PAN field of the authorization request message contains an encrypted PAN.

9. A method comprising:

receiving, by a host server, an authorization request message, wherein the authorization request message includes an encrypted PIN that was encrypted using a first encryption key variant based on an initial key, and encrypted sensitive data that was encrypted using a second encryption key variant based on the initial key;

decrypting, by a secure module communicatively connected to the host server, the encrypted sensitive data;

re-encrypting, by the secure module, the decrypted sensitive data, wherein the sensitive data re-encryption uses a first sensitive data zone encryption key associated with the first payment processing network; and

transmitting, by the host server, a first translated authorization request message to the first payment processing network, wherein the translated authorization request message includes the re-encrypted sensitive data.

10. The method of claim 9, further comprising:

decrypting, by the secure module, the encrypted PIN; and

re-encrypting, by the secure module, the decrypted PIN, wherein the PIN re-encryption uses a first PIN zone encryption key associated with a first payment processing network; and

wherein the first translated authorization request message includes the re-encrypted PIN.

11. The method of claim 10, wherein the secure module is configured to transmit a second translated authorization request message to a second payment processing network, wherein a second PIN zone encryption key is used for re-encryption a PIN for the second translated authorization request message and a second sensitive data zone encryption key is used for re-encryption of sensitive data for the second authorization request message.

12. The method of claim 9, wherein the initial key is generated by a derived unique key per transaction (DUKPT) key management scheme.

13. The method of claim 9, wherein the decrypting of the encrypted sensitive data, and the re-encrypting of the decrypted sensitive data are performed by a hardware security module acting as the secure module.

14. The method of claim 9, wherein the sensitive data includes at least one of a primary account number (PAN), a cardholder name, a cardholder address, and discretionary data.

15. A system comprising:

a processor; and

a computer readable medium coupled to the processor, wherein the computer readable medium comprises code executable by the processor for implementing a method of routing transactions, the method comprising:

encrypting, by an access device, a personal identification number (PIN), wherein the PIN encryption uses a first encryption key variant based on an initial key;

encrypting, by the access device, sensitive data, wherein the sensitive data encryption uses a second encryption key variant based on the initial key; and

transmitting, to a host server, an authorization request message including the encrypted PIN and encrypted sensitive data.

16. A system comprising:

a processor; and

a computer readable medium coupled to the processor, wherein the computer readable medium comprises code executable by the processor for implementing a method comprising:

receiving, by a host server, an authorization request message, wherein the authorization request message includes an encrypted PIN that was encrypted using a first encryption key variant based on an initial key, and encrypted sensitive data that was encrypted using a second encryption key variant based on the initial key;

decrypting, by a secure module communicatively connected to the host server, the encrypted sensitive data;

re-encrypting, by the secure module, the decrypted sensitive data, wherein the sensitive data re-encryption uses a first sensitive data zone encryption key associated with the first payment processing network; and

transmitting, by the host server, a first translated authorization request message to the first payment processing network, wherein the translated authorization request message includes re-encrypted sensitive data.

17. The method of claim 16, further comprising:

decrypting, by the secure module, the encrypted PIN; and

re-encrypting, by the secure module, the decrypted PIN, wherein the PIN re-encryption uses a first PIN zone encryption key associated with a first payment processing network; and

wherein the first translated authorization request message includes the re-encrypted PIN.

18. The system of claim 16, wherein the secure module is configured to transmit a second translated authorization request message to a second payment processing network, wherein a second PIN zone encryption key is used for re-encryption of a PIN for the second translated authorization request message and a second sensitive data zone encryption key is used for re-encryption of sensitive data for the second authorization request message.

19. The system of claim 16, wherein the system includes a hardware security module.

20. A method, comprising:

receiving data associated with a personal account identifier (PAI)

encrypting, by the access device, the PAI, wherein the encrypted PAI has the same format as the PAI;

writing the encrypted PAI to a field of an authorization request message, wherein the field is designated to receive a PAI;

using an authorization request message data element as a signal to identify the presence of the encrypted PAI in the authorization request message; and

transmitting the authorization request message.

21. The method of claim 20, wherein the PAI is a primary account number (PAN), wherein a subset of digits of the encrypted PAN in the authorization request message are unencrypted digits of the PAN.

22. The method of claim 20, wherein the first six digits of the encrypted PAN are the same as the first six digits of the unencrypted PAN and wherein the last four digits of the encrypted PAN are the same as the last six digits of the unencrypted PAN.

23. The method of claim 21, further comprising calculating a value for a designated digit of the encrypted PAN such that the last digit of the unencrypted PAN is the

same as the last digit of the encrypted PAN and wherein the last digit of the encrypted PAN is a valid check digit for the encrypted PAN.

24. The method of claim 20, wherein the authorization request message includes an expiration date, and wherein the expiration date field of the authorization request message is overwritten with an altered expiration date when the PAI field of the authorization request message contains an encrypted PAI.