Office de la Propriété Intellectuelle du Canada
Un organisme d'Industrie Canada

Canadian Intellectual Property Office
An agency of Industry Canada

CA 2655465 C 2017/03/07

(11)(21) **2 655 465**

(12) **BREVET CANADIEN**
CANADIAN PATENT

(13) **C**

(86) **Date de dépôt PCT/PCT Filing Date:** 2007/06/14
(87) **Date publication PCT/PCT Publication Date:** 2007/12/27
(45) **Date de délivrance/Issue Date:** 2017/03/07
(85) **Entrée phase nationale/National Entry:** 2008/12/15
(86) **N° demande PCT/PCT Application No.:** US 2007/071200
(87) **N° publication PCT/PCT Publication No.:** 2007/149762
(30) **Priorités/Priorities:** 2006/06/19 (US60/815,059); 2006/06/20 (US60/815,430); 2007/01/09 (US60/884,089)

(51) **Cl.Int./Int.Cl.** ***G06Q 20/40*** (2012.01), ***H04L 9/32*** (2006.01)

(72) **Inventeur/Inventor:**
HAMMAD, AYMAN, US

(73) **Propriétaire/Owner:**
VISA U.S.A. INC., US

(74) **Agent:** FETHERSTONHAUGH & CO.

(54) **Titre : CRYPTAGE DE DONNEES DE SUIVI**
(54) **Title: TRACK DATA ENCRYPTION**

PAN	EXP DATE	SERVICE CODE	PIN VERIFICATION DATA	CVV+	DISC DATA

(57) **Abrégé/Abstract:**
A method for using a secondary PAN is disclosed. The method includes providing a secondary PAN associated with a primary PAN, where the secondary PAN has at least one end portion that is the same as the primary PAN, but has a middle portion of that is different than the primary PAN.

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

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
27 December 2007 (27.12.2007)

PCT

(10) International Publication Number
WO 2007/149762 A3

(51) International Patent Classification:
H04K 1/00 (2006.01)

(21) International Application Number:
PCT/US2007/071200

(22) International Filing Date: 14 June 2007 (14.06.2007)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:

60/815,059	19 June 2006 (19.06.2006)	US
60/815,430	20 June 2006 (20.06.2006)	US
60/884,089	9 January 2007 (09.01.2007)	US

(71) Applicants *(for all designated States except US)*: **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; 900 Metro Center Boulevard, Foster City, California 94404 (US). **VISA U.S.A. INC.** [US/US]; P.O. Box 8999, San Francisco, California 94128 (US).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: **HAMMAD, Ayman** [US/US]; 6048 Corte Montanas, Pleasanton, California 94566 (US).

(74) Agents: **JEWIK, Patrick, R.** et al.; Townsend and Townsend and Crew LLP, Two Embarcadero Center, 8th Floor, San Francisco, California 94111-3834 (US).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, 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.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IS, IT, LT, LU, LV, MC, MT, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:
— *with international search report*

(88) Date of publication of the international search report:
21 February 2008

(54) Title: TRACK DATA ENCRYPTION

PAN	EXP DATE	SERVICE CODE	PIN VERIFICATION DATA	CVV+	DISC DATA

(57) Abstract: A method for using a secondary PAN is disclosed. The method includes providing a secondary PAN associated with a primary PAN, where the secondary PAN has at least one end portion that is the same as the primary PAN, but has a middle portion of that is different than the primary PAN.

WO 2007/149762 A3

TRACK DATA ENCRYPTION

BACKGROUND

[0001] In a typical purchase transaction, a consumer may use a portable consumer device to buy goods or services from a merchant. The consumer's PAN or primary account number may be stored in a memory on the portable consumer device.

[0002] The PAN may be read at a point of sale terminal operated by a merchant, and the PAN and other information may be transmitted to the issuer of the portable consumer device along with other transaction information such as the amount of the purchase, etc. Once received, the issuer may then decide whether or not the consumer is authorized or not authorized to conduct the purchase transaction.

[0003] In conventional purchase transactions, the PAN is not encrypted when it passes from the portable consumer device, to the point of sale terminal, and to the issuer. The non-encryption of the PAN is not a major issue in view of current network security and fraud detection mechanisms. However, it would be desirable to add upfront security to existing payment systems. For example, if the PAN gets intercepted by an unauthorized person during the transmission of the PAN from the point of sale terminal to the issuer, the unauthorized person could use the PAN to make unauthorized purchases. Thus, new ways to provide for secure transmission of the PAN to the issuer or other entity are desirable.

[0004] Embodiments of the invention address these and other problems individually and collectively.

SUMMARY

[0005] Embodiments of the invention are directed to methods, systems, and computer readable media that can be used to securely deliver a PAN associated with a portable consumer device from a portable consumer device, a point of sale terminal, or some other location, to an issuer of the portable consumer device.

[0006] The real PAN associated with the consumer and the consumer's portable consumer device may be referred to as a "primary PAN." In embodiments of the invention, the primary PAN can be changed to a secondary PAN, which is linked to the primary PAN. At least a portion of the secondary PAN may be changed (e.g., encrypted) before it arrives at the issuer, and the issuer (or other entity such as a payment processing network) may subsequently determine the consumer's primary PAN from the received secondary PAN. The secondary PAN mayor may not be known to the consumer.

[0007] Advantageously, the secondary PAN can be used to securely transmit primary PAN information to the issuer. Also, the secondary PAN may be used to authenticate the portable consumer device being used in a particular transaction. If, for example, the secondary PAN that is received by the issuer is not the correct secondary PAN (e.g., the issuer expects to receive the secondary PAN, and not the primary PAN, in Track 1 or Track 2), then the issuer may conclude that the portable consumer device being used is not authentic and may thereafter not approve the payment transaction.

[0008] One embodiment of the invention is directed to a method comprising providing a secondary PAN associated with a primary PAN, wherein the secondary PAN has end portions, and at least one end portion (e.g., a BIN or bank identification number end portion) is the same as the primary PAN. The secondary PAN may also have a middle portion that is different than the primary PAN. Approval or disapproval for a payment transaction is received after providing the secondary PAN. This method may be performed by any suitable entity including the consumer or the merchant, with or without other entities.

[0009] Another embodiment of the invention is directed to a portable consumer device comprising a body, and a computer readable medium coupled to

the body. The computer readable medium comprises code for a secondary PAN associated with a primary PAN. The secondary PAN has end portions, and at least one of the end portions is the same as the primary PAN. A middle portion of secondary PAN is different than the primary PAN.

[0010] Another embodiment of the invention is directed to a computer readable medium. The computer readable medium comprises code for providing a secondary PAN associated with a primary PAN using a portable consumer device. The secondary PAN has end portions, and at least one end portion is the same as the primary PAN. The secondary PAN also has a middle portion that is different than the primary PAN. The computer readable medium also comprises code for receiving approval or disapproval for a payment transaction after providing the secondary PAN.

[0011] Another embodiment of the invention is directed to a method comprising receiving an authorization request message associated with a transaction, the authorization request message including a secondary PAN associated with a primary PAN. The secondary PAN has end portions and a middle portion. At least one of the end portions is the same as the primary PAN, and at least a middle portion of the secondary PAN is different than the primary PAN. Once the secondary PAN is received, the secondary PAN is analyzed, and the primary PAN is analyzed after analyzing the secondary PAN. After the primary and secondary PANs are analyzed, an authorization response message is sent. The authorization response message indicates approval or disapproval of the transaction. This method may be performed by one or more entities including an issuer, payment processing network, etc.

[0012] Another embodiment of the invention is directed to a computer readable medium. The computer readable medium comprises code for receiving an authorization request message associated with a transaction, where the authorization request message including a secondary PAN associated with a primary PAN. The secondary PAN has end portions, and at least one of the end portions is the same as the primary PAN. A middle portion of the secondary PAN is different than the primary PAN. The computer readable medium also comprises code for analyzing the secondary PAN, code for analyzing the primary PAN, and code for

sending an authorization response message, wherein the authorization response message indicates approval or disapproval of the transaction.

[0013] Another embodiment of the invention is directed to a method comprising providing a secondary PAN associated with a primary PAN, wherein the secondary PAN has a location identification data element. The location identification data element is the same in both the primary and secondary PANs, and at least the middle portion of the secondary PAN is different than the primary PAN. The method also includes receiving approval or disapproval for a payment transaction after providing the secondary PAN.

[0013a] In another illustrative embodiment, a method includes receiving, at a server computer, an authorization request message associated with a transaction. The authorization request message includes a secondary PAN associated with a primary PAN. The secondary PAN is within a PAN field of the authorization request message. The primary PAN includes a primary PAN first end portion and a primary PAN second end portion, and the secondary PAN includes a secondary PAN first end portion and a secondary PAN second end portion, the secondary PAN second end portion being the same as the primary PAN second end portion. The method further includes determining, by the server computer, that the secondary PAN is not a valid primary account number. Based on the determining that the secondary PAN is not valid, the method further includes obtaining, by the server computer, the primary PAN based upon data at another location outside the PAN field of the authorization request message. The method further includes determining, by the server computer based upon the primary PAN, whether the transaction is authorized, and sending an authorization response message that indicates an approval of the transaction or a disapproval of the transaction.

[0013b] In another illustrative embodiment, a computer readable medium stores instructions which, when executed by a processor, cause the processor to perform operations including receiving an authorization request message associated with a transaction. The authorization request message includes a secondary PAN associated with a primary PAN. The secondary PAN is within a PAN field of the authorization request message. The primary PAN includes a primary PAN first end portion and a primary PAN second end portion, and the secondary PAN includes a secondary PAN

first end portion and a secondary PAN second end portion, the secondary PAN second end portion being the same as the primary PAN second end portion. The instructions further cause the processor to determine that the secondary PAN is not a valid primary account number. Based on the determining that the secondary PAN is not valid, the instructions further cause the processor to obtain the primary PAN based upon data at another location outside the PAN field of the authorization request message, to determine, based upon the primary PAN, whether the transaction is authorized, and to send an authorization response message that indicates an approval of the transaction or a disapproval of the transaction.

[0013c] In another illustrative embodiment, a server computer includes a processor and a computer readable medium storing instructions which, when executed by the processor, cause the server computer to perform operations including receiving an authorization request message associated with a transaction, wherein the authorization request message includes a secondary PAN associated with a primary PAN, and the secondary PAN is within a PAN field of the authorization request message. The primary PAN includes a primary PAN first end portion and a primary PAN second end portion, and the secondary PAN includes a secondary PAN first end portion and a secondary PAN second end portion, the secondary PAN second end portion being the same as the primary PAN second end portion. The operations further include determining that the secondary PAN is not a valid primary account number. Based on the determining that the secondary PAN is not valid, the operations further include obtaining the primary PAN based upon data at another location outside the PAN field of the authorization request message, determining, based upon the primary PAN, whether the transaction is authorized, and sending an authorization response message that indicates an approval of the transaction or a disapproval of the transaction.

[0014] These and other embodiments of the invention are described in further detail below, with reference to the Figures.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] FIG. 1 shows a schematic illustration of data elements in a data track associated with a portable consumer device.

[0016] FIG. 2 shows a Track 2 data track as read from an MSD (magnetic stripe data) chip card.

[0017] FIG. 3 shows a Track 2 data track as read from a magnetic stripe card.

[0018] FIG. 4 shows a system according to an embodiment of the invention.

[0019] FIG. 5 shows a flowchart illustrating a method according to an embodiment of the invention.

[0020] FIGS. 6(a)-6(b) show primary and secondary PANs that can be used in the method shown in FIG. 5.

[0021] FIG. 7 shows a flowchart illustrating another method according to an embodiment of the invention.

[0022] FIG. 8 shows a schematic illustration of a secondary PAN.

DETAILED DESCRIPTION

[0023] As explained above, a consumer's PAN is not encrypted in conventional purchase transactions. While encryption of the entire PAN can be contemplated to enhance security, encrypting the entire PAN may not be practical under all circumstances. For example, the PAN contains a BIN or a bank identification number. The BIN is used to route the transaction data to the issuer, and the encrypted BIN may not be recognized by the routing and switching infrastructure computers that route transaction data to the issuer. If the entire PAN is encrypted, then the BIN would change and this would cause routing problems. Accordingly, any encryption process that is used to encrypt the PAN would preferably do so without negatively impacting the existing payments infrastructure, and the way that payment transactions are currently handled.

[0024] There are a number of other restrictions associated with encrypting PANs. For example, in the context of a payment card with a magnetic stripe, cardholder account data (including the cardholder's PAN) on the magnetic stripe is encoded on "Track 1" and/or "Track 2" of the magnetic stripe. Track 1 ("International Air Transport Association") stores more information than Track 2, and contains the cardholder's name as 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. The ABA (American Banking Association) designed the specifications of this track and all world banks must abide by it. It contains the cardholder's account, encrypted PIN, plus other discretionary data.

[0025] Track 1 is 79 characters long and has limited space. Track 2 is a totally numeric field, is 37 characters long, and also has limited space. Because of these restrictions, the data that are in Track 1 or Track 2 are in decimal form. The data cannot be in any other form such as hexadecimal (except for the cardholder name in track1). This limits the ability to encrypt the PAN in Tracks 1 or 2.

[0026] FIG. 1 shows a generic schematic diagram representing a generic data track associated with a portable consumer device. The illustrated data track contains various data fields. As shown in FIG. 1, the data fields may contain a PAN

field, an expiration date field, a service code field, a PIN, a CVV (personal identification number card verification value) field, and discretionary data fields. Typical PANs may be between about 13-19 digits (e.g., 13, 16, or 19 digits) long, and the PAN data field may be configured to store data of a corresponding size.

[0027] FIG. 2 shows a specific example of a Track 2 format as read from an MSD (magnetic stripe data) chip card. As shown, the exemplary Track 2 format includes a PAN **390**, a separator **392**, an expiration date **394**, a PVKI (pin verification key indicator) **398**, pin verification data **400**, a dCVV (dynamic card verification value) **402**, an ATC (automatic transaction counter **404**, a contactless indicator **406** in an issuer discretionary data field or IDD data field, and padding **408**.

[0028] FIG. 3 shows an exemplary Track 2 data track as read from a magstripe or magnetic stripe card. In FIG. 3, there is a start sentinel **414**, and a separator **416**. The BIN is between the start sentinel **414** and the separator **416**. There is also an end sentinel **418**, and a checksum to the right of the end sentinel **420**.

[0029] The data tracks in FIGS. 1 and 2 are slightly different. The magstripe Track 2 data track shown in FIG. 3 uses an end sentinel **420**, since a magnetic reader head in a point of sale terminal would need to know when to start and stop reading data. By comparison, in the chip card Track 2 data track shown in FIG. 2, an end sentinel is not necessary, since the chip in the chip card would output the appropriate amount of data to the point of sale terminal.

[0030] Another restriction on encrypting a PAN is that the length of PANs may vary in different countries. For example, PANs may be 13, 16, or 19 digits long. Any method and system for encrypting PANs would preferably work with PANs of varying length.

[0031] Another restriction on encrypting a PAN is that the last digit of the PAN is a check digit. It is used to ensure the data integrity of the PAN as it is read by the point of sale terminal. A check digit is a digit added to a number (either at the end or the beginning) that validates the authenticity of the number. A simple algorithm is applied to the other digits of the number which yields the check digit. By running the algorithm, and comparing the value that is determined by the algorithm with the check digit value at the end of the PAN, one can verify that all of the digits are

correctly read and that they make a valid combination. A commonly used, well known check digit algorithm is a called a "mod 10" algorithm.

[0032] The encryption processes according to embodiments of the invention can be used despite the above-noted restrictions. Embodiments of the invention protect the consumer's PAN and can be used with existing payment verification mechanisms and systems. As will be illustrated in further detail below, embodiments of the invention can encrypt a PAN without requiring any major or unexpected changes to the existing payments infrastructure. Also, embodiments of the invention can also be used with PANs of varying length.

[0033] Embodiments of the invention partially "mask" the primary PAN by creating a secondary PAN that is linked to the primary PAN. In one embodiment of the invention, a portion of a transmitted PAN is masked and/or changed by an access device (e.g., a point of sale terminal), a portable consumer device, or the like, before it is received by the issuer during a transaction such as a payment transaction. The portion that is changed (e.g., encrypted) is preferably the middle portion of the PAN. The middle portion may be of any suitable length, but is preferably between 3 and 9 digits long.

[0034] Any suitable encryption process may be used to mask the middle portion of the PAN. For example, embodiments of the invention may use DES (dynamic encryption standard), ECC (elliptical curve cryptography), or AEC (advanced encryption cryptography) processes. Any symmetric or asymmetric cryptographic elements may be used.

[0035] There are two end portions (e.g., each 4-6 digits long) on opposite sides of the middle portion of the PAN, and at least one of the end portions remains static during the transaction process. For example, at least one end portion of the PAN, which includes the BIN or bank identification number, remains static during the transaction process and at least the middle portion is changed or encrypted. The BIN (or other location identification data element) remains static during the transaction process so that the PAN and other transaction data can be routed to the issuer. The BIN typically occupies the first six digits of the PAN and may be considered a first end portion of the PAN. In other embodiments, instead of a BIN, the merchant location identifier, financial institution location identifier, or even an IP

address could be in an end portion of the PAN and may remain static. Any of these may remain static in the PAN instead of the BIN.

[0036] In addition to the first end portion of the PAN including the BIN, the other end portion of the PAN also preferably remains static during the transaction process. The second end portion of the primary PAN that remains static preferably includes the last four digits of the primary PAN. That is, the last four digits of the primary and secondary PANs are the same.

[0037] There are a number of advantages associated with keeping the second end portion of the secondary PAN the same as the primary PAN. As noted above, the last character of the primary PAN is a check digit or a mod 10 calculation to ensure data integrity. It is therefore desirable that at least this last check digit not be changed so that the point of sale terminal still performs the appropriate check sum verification process. Lastly, the consumer is used to seeing the last four digits of the PAN printed on the consumer's purchase receipts, so it would be desirable not to change the last four digits of the PAN. In addition, the last four digits of the PAN are typically printed on purchase receipts which are often discarded by consumers, so the last four digits are easily discovered. There is therefore little benefit in encrypting the last four digits of the primary PAN. Thus, in preferred embodiments of the invention, the dynamically changing numbers of the PAN are typically masked. The last four digits are static on a payment card receipt that is received by a consumer so that the consumer advantageously does not see anything unusual.

[0038] FIG. 1 shows a system **20** that can be used in an embodiment of the invention. The system **20** includes a merchant **22** and an acquirer **24** associated with the merchant **22**. In a typical payment transaction, a consumer **30** may purchase goods or services at the merchant **22** using a portable consumer device **32**. The acquirer **24** can communicate with an issuer **28** via a payment processing network **26**.

[0039] The acquirer **24** is typically a bank that has a merchant account. The issuer **28** may also be a bank, but could also be business entity such as a retail store. Some entities are both acquirers and issuers, and embodiments of the invention include such entities.

[0040] The consumer **30** may be an individual, or an organization such as a business that is capable of purchasing goods or services.

[0041] The portable consumer device **32** may be in any suitable form. For example, suitable portable consumer devices can be hand-held and compact so that they can fit into a consumer's wallet and/or pocket (e.g., pocket-sized). They may include smart cards, ordinary credit or debit cards (with a magnetic strip and without a microprocessor), keychain devices (such as the Speedpass™ commercially available from Exxon-Mobil Corp.), etc. Other examples of portable consumer devices include cellular phones, personal digital assistants (PDAs), pagers, payment cards, security cards, access cards, smart media, transponders, and the like. The portable consumer devices can also be debit devices (e.g., a debit card), credit devices (e.g., a credit card), or stored value devices (e.g., a stored value card).

[0042] The portable consumer device **32** may comprise a computer readable medium **32(a)** and a body **32(b)**. The computer readable medium **32(a)** may be on the body **32(b)**, which may in the form a plastic substrate, housing, or other structure. If the portable consumer device **32** is in the form of a card, it may have an embossed region **32(c)** which is embossed with the primary PAN.

[0043] The computer readable medium **32(a)** may be a memory that stores data and may be in any suitable form. Exemplary computer readable media **32(a)** may be in the form of a magnetic stripe, a memory chip, etc. The computer readable medium **32(a)** may electronically store the primary and/or the secondary PAN in encrypted or unencrypted form.

[0044] The payment processing network **26** may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. An exemplary payment processing network may include VisaNet™. Payment processing networks such as VisaNet™ are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes a VIP system (Visa Integrated Payments system) which processes authorization requests and a Base II system which performs clearing and settlement services.

[0045] The payment processing network **26** may include a server computer. A server computer is typically a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server. The payment processing network **26** may use any suitable wired or wireless network, including the Internet.

[0046] The merchant **22** may also have, or may receive communications from, an access device **34** that can interact with the portable consumer device **32**. In FIG. 4, the access device **34** is located at the merchant **22**. However, it could be located at any other suitable location in other embodiments of the invention.

[0047] The access devices according to embodiments of the invention can be in any suitable form. Examples of access devices include point of sale (POS) devices, cellular phones, PDAs, personal computers (PCs), tablet PCs, handheld specialized readers, set-top boxes, electronic cash registers (ECRs), automated teller machines (ATMs), virtual cash registers (VCRs), kiosks, security systems, access systems, and the like.

[0048] The access device **34** may include a reader **34(a)**, a processor **34(b)** and a computer readable medium **34(c)**. The reader **34(b)** may use any suitable contact or contactless mode of operation. For example, exemplary card readers can include RF (radio frequency) antennas, magnetic stripe readers, etc. to interact with the portable consumer device **32**.

[0049] In a typical purchase transaction, the consumer **30** purchases a good or service at the merchant **22** using a portable consumer device **32** such as a credit card. The consumer's portable consumer device **32** can interact with an access device **34** such as a POS (point of sale) terminal at the merchant **22**. For example, the consumer **30** may take a credit card and may swipe it through an appropriate slot in the POS terminal. Alternatively, the POS terminal may be a contactless reader, and the portable consumer device **32** may be a contactless device such as a contactless card.

[0050] An authorization request message is then forwarded to the acquirer **24**. After receiving the authorization request message, the authorization request message is then sent to the payment processing network **26**. The payment

processing network **26** then forwards the authorization request message to the issuer **28**, or a third party entity acting on behalf of the issuer, of the portable consumer device **32**.

[0051] After the issuer **28**, or a third party entity acting on behalf of the issuer, receives the authorization request message, the issuer **28**, or the third party entity acting on behalf of the issuer, sends an authorization response message back to the payment processing network **26** to indicate whether or not the current transaction is authorized (or not authorized). The transaction processing network **26** then forwards the authorization response message back to the acquirer **24**. The acquirer **24** then sends the response message back to the merchant **22**.

[0052] After the merchant **22** receives the authorization response message, the access device **34** at the merchant **22** may then provide the authorization response message for the consumer **30**. The response message may be displayed by the access device **34**, or may be printed out on a receipt.

[0053] At the end of the day, a normal clearing and settlement process can be conducted by the transaction processing network **26**. A clearing process is a process of exchanging financial details between and acquirer and an issuer to facilitate posting to a consumer's account and reconciliation of the consumer's settlement position.

[0054] Embodiments of the invention can utilize secondary PANs in the above-described payment transaction processes. Such embodiments are described below with reference to FIGS. 4-8.

[0055] An encryption method according to one embodiment of the invention may be described with reference to FIGS. 4, 5 and 6(a)-6(b).

[0056] In an exemplary embodiment, a consumer **30** uses his portable consumer device **32** to pay for goods or services offered by the merchant **22**. The consumer **30** takes the portable consumer device **32** and uses it to interact with the reader **34(a)** in the access device **34** as described above. The primary PAN may be stored in the computer readable medium **32(a)**.

[0057] The access device **34** can then receive the primary PAN from the portable consumer device **32** (step **502**). The primary PAN may be received from

the portable consumer device **32** using any suitable contact or contactless mode of operation.

[0058] Once the processor **34(b)** in the access device **34** receives the primary PAN, it can take the primary PAN and can change the middle portion of the PAN, while at least one end portion remains static to produce a secondary PAN (step **504**). Preferably, both end portions including the BIN and the last four digits of the PAN are the same in both the primary and secondary PANs. For example, FIG. 6(a) shows an exemplary primary PAN which is "4592341234563337." The first six digits "459234" represent the BIN, may be a first end portion, and are static (i.e., the first six digits are the same in both the primary and secondary PANs) during the transaction process. The last four digits "3337" may constitute a second end portion and may also remain static (i.e., the last four digits are the same in both the primary and secondary PANs) during the transaction process. In this example, the first end portion of the secondary PAN (or the primary PAN) includes six digits while the second end portion includes four digits. In other embodiments, the first and second end portions, and the middle portion, may include more or less digits.

[0059] While the first and second end portions remain static, at least a majority of the digits in the middle portion are changed. Preferably, at least 3, 4, or 5 digits in the middle portion, all of the digits in the middle portion, or all of the digits except for one digit in the middle portion, are changed so that they are all the same. For example, as shown in FIG. 6(b), the middle six digits are "zeroed" out in a secondary PAN. By doing this, the issuer can be assured that the formed secondary PAN is not the same as a primary PAN that is associated with another consumer. After the issuer receives the secondary PAN, the issuer would recognize that there is no account number with six zeros in the middle, and the issuer would then locate the primary PAN at another location (as described in further detail below).

[0060] In some embodiments, all digits in the middle portion of the secondary PAN are the same, except for one digit. The one digit that is not the same as the other digits may be adjusted so that when a checksum calculation is performed on the secondary PAN, it will match the checksum digit in the primary PAN (i.e., the last digit of the PAN). For example, a checksum calculation may result in "7" for a primary PAN and the number "7" may be at the end of the primary PAN. If all digits

in the middle portion of the primary PAN are changed to "0" to form a secondary PAN, this may result in a different checksum value. For example, after replacing the middle portion of the primary PAN with zeros, the checksum value may be different than "7". However, to "trick" the access device **22** into thinking that the correct PAN has been received, one digit in the middle portion of the PAN may be changed to a number other than zero so that the result of the checksum calculation is the proper one. For example, referring to FIG. 6(b), the middle portion of the secondary PAN may be changed to "000900." The addition of the number "9" to the middle portion may cause a checksum calculation to produce the same result (e.g., "7") as the checksum digit associated with an unaltered primary PAN (e.g., "7").

[0061] After the secondary PAN is created, the processor **34(b)** then stores the secondary PAN in a location where the primary PAN is normally located (e.g., Track 2). The processor **34(b)** may then encrypt the entire primary PAN or just a portion of the primary PAN (step **508**). The encrypted primary PAN may then be stored in an area other than the data track from which it came (step **510**), or in a location other than where it is normally stored. For example, if the primary PAN was originally stored in Track 2, then the encrypted primary PAN may be stored in Track 3 or some other area. The processor **34(b)** may perform these and other functions and code for causing the processor **34(b)** to perform these functions may be stored in the computer readable medium **34(c)**.

[0062] The access device **34** may then send both the encrypted primary PAN and the secondary PAN (with or within an authorization request message) to the issuer **28** via the acquirer **24** and the payment processing network **26** (step **512**). The issuer **28** may then receive both the encrypted primary PAN and secondary PAN (step **514**).

[0063] A server computer **21** at the issuer **28** then analyzes the secondary PAN (step **516**), and then checks to see if it matches the account numbers of any of its customers. Because the middle portion of the secondary PAN has a majority of its digits repeated, or because a valid PAN structure is not present, the server computer **21** at the issuer **28** will recognize that the secondary PAN does not match of its existing account numbers. Consequently, the server computer **21** can then look to the area where the encrypted primary PAN is stored. The server computer

28 then locates the encrypted primary PAN and then decrypts the primary PAN **518** using a key that is stored in the database **23**. Once the primary PAN **518** is decrypted, it is analyzed and the portable consumer device **32** is thereafter authenticated. After authenticating the portable consumer device **32**, the issuer **28** sends the authorization response message back to the merchant **22** indicating whether or not the consumer **30** is authorized to conduct the transaction.

[0064] Although one issuer **28** is shown in FIG. 1, in embodiments of the invention, there may be many issuers. Each issuer can determine the area where the primary PAN is to be stored, if it wants to encrypt the primary PAN in that stored area, and/or the key that is used to encrypt the primary PAN. If different issuers use different protocols for storing and processing the primary PAN, then the risk of widespread fraudulent activity is reduced. For example, if the data that is being transmitted from the merchant **22** to the issuer **28** is intercepted by an unauthorized person, and if the unauthorized person is even capable of determining where the encrypted primary PAN is stored and how to decrypt the transmitted data, the unauthorized person would not be able to use this information to intercept and decrypt PAN information passing to other issuers, since the other issuers would be using a different data protection protocol than the issuer **28**.

[0065] In the above described example, the secondary PAN is created at the access device **34**. Thus, data transmission is very secure between the access device **34** and the issuer **28**. However, the secondary PAN could also be generated at any other suitable location. For example, to provide even more security, the portable consumer device **32** could provide both the primary and second PANs to the access device **34** so that the access device **34** does not perform any data conversions or encryption of the primary PAN. The secondary PAN may be stored statically on the computer readable medium **32(a)** of the portable consumer device **32**, or may be dynamically generated by the portable consumer device **32** if the portable consumer device **30** is a smart card or the like. In such embodiments, the secure transmission of the primary PAN can be provided from the portable consumer device **32** to the issuer **28** to authenticate the portable consumer device **32**.

[0066] Other embodiments of the invention can be described with reference to FIGS. 4, 7 and 8.

[0067] FIG. 7 shows a flowchart illustrating an embodiment of the invention. As in the previously described embodiments, in this embodiment, a consumer **30** uses his portable consumer device **32** to pay for goods or services offered by the merchant **22**. The consumer **30** takes the portable consumer device **32** and uses it to interact with the reader **34(a)** in the access device **34**. The primary PAN may be stored in the computer readable medium **32(b)**.

[0068] The access device **34** then receives the primary PAN from the portable consumer device **32** (step **602**). The primary PAN may be received from the portable consumer device **32** using any suitable contact or contactless mode of operation.

[0069] Once the processor **34(b)** in the access device **34** receives the primary PAN, it can take the primary PAN and can change the middle portion of the PAN, while at least one end portion remains static, to produce a secondary PAN (step **604**). For example, FIG. 8 shows a schematic illustration of a 16 digit PAN **380** that might reside in the computer readable medium **32(a)** (e.g., a magnetic stripe) in the portable consumer device **32**. In this example, the first six digits (i.e., a first end portion) "123456" **380(a)** of the PAN **380** would correspond to the BIN number. The next 6 digits **380(b)** may be changed or different from the real PAN's 6 digits and are represented by "XXXXXX" in this example. In a preferred embodiment, the middle six digits may be dynamically changed using a counter or the like. This makes it more difficult for any unauthorized person to determine the primary PAN.

[0070] The last four digits **380(c)** (i.e., a second end portion) are "9999" in this example, and would remain the same. By keeping the BIN and the last four digits the same, the transaction will look like a real one to the merchant and the consumer.

[0071] In this embodiment, the middle portion does not intentionally contain repeating numerical values, so the issuer **28** may take steps to ensure that the secondary PAN does not match or overlap with the primary PANs of other customers. For example, the issuer may set aside a set of numbers specifically reserved for secondary PANs, and not primary PANs.

[0072] The access device **34** then optionally encrypts the secondary PAN (step **608**) and sends the encrypted secondary PAN to the issuer **28** via the acquirer **24** and the payment processing network **26** (step **610**). The issuer **28** then receives

the encrypted secondary PAN (step **614**), decrypts it (step **616**), determines the primary PAN, and then analyzes it (step **618**). An appropriate algorithm or look-up table (e.g., stored in the database **23**) at the issuer **28** may be used to link the primary and secondary PANs. After the issuer **28** determines the primary PAN, the issuer **28** may then authenticate the portable consumer device **32** (step **620**). The issuer **28** thereafter sends an authorization response message back to the merchant **22** via the payment processing network **26** and the acquirer **24** indicating whether or not the transaction is authorized or approved (step **622**).

[0073] In many of the specific embodiments described above, a secondary PAN and/or primary PAN is encrypted by an access device **34**, a portable consumer device **32**, or the like. The encrypted secondary PAN and/or primary PAN is received at the issuer **28** and the issuer **28** may then decrypt the secondary PAN and/or the primary PAN to authenticate the portable consumer device **32** and process the payment transaction. It is understood, however, that in other embodiments of the invention, the decryption process may occur at the payment processing network **26**, before the PANs arrive at the issuer **28** in a similar manner as described above. For example, after the primary PAN and/or secondary PAN are decrypted by the payment processing network **26**, the payment transaction process can proceed as it normally does. That is, the payment processing network **26** can receive the encrypted primary PAN and/or secondary PAN, decrypt them, verify that the portable consumer device **32** is authentic, and then reformat the authorization request message in a normal format so that the decrypted primary PAN is located in an area where it is normally located. After the authorization request message is reformatted, it can be sent to the issuer **28** as it would be sent in a conventional manner. The issuer **28** can then send the payment processing network **26** an authorization response message, and the payment processing network **26** may in turn send it back to the access device **34** via the acquirer **24** and the merchant **22**. Such embodiments are advantageous, since security is enhanced compared to conventional payment processes, yet the issuer **28** will see the same transaction information that it normally sees in conventional payment processes.

[0074] Also, in many of the embodiments described above, the secondary PAN is generated during the transaction process. This is not necessary in all cases. Instead of generating the secondary PAN at the access device **34**, the secondary

PAN may be stored in the computer readable medium of the portable consumer device and it may have a middle portion that is different than the middle portion of the primary PAN. In such embodiments, the secondary PAN may not be generated during the particular transaction being conducted, but may have been previously generated and stored on the portable consumer device **32**. In some cases, the primary PAN and may be embossed on the portable consumer device **32** if the portable consumer device **32** is in the form of a payment card, and the secondary PAN may be stored in the computer readable medium **32(a)** in the portable consumer device **32**.

[0075] As illustrated above, in some embodiments, both the primary PAN and the secondary PAN may be transmitted to the issuer to verify that the portable consumer device being used is authentic. If an unauthorized person tries to use the primary PAN, then that unauthorized person will not know the secondary PAN and cannot fraudulently conduct a purchase transaction without knowing the secondary PAN. Alternatively, if an unauthorized person electronically intercepts or "skims" the secondary PAN, then the unauthorized person will not be able to conduct the purchase transaction without knowing the primary PAN.

[0076] In yet other embodiments, as noted above, the middle portion of the PAN may be changed dynamically. For example, an appropriate algorithm or counter may be used to dynamically change the middle portion of the PAN each time the portable consumer device is used. This way, even if the primary PAN is electronically intercepted by an unauthorized person, and the unauthorized person knows the primary PAN, the secondary PAN will be dynamically changing. Even if the unauthorized person knows the primary PAN and intercepts the secondary PAN once, the intercepted secondary PAN would be useless, since it is a dynamically changing secondary PAN. In this case, the unauthorized person would need to know the algorithm used to dynamically change the PAN in addition to the primary PAN, the secondary PAN and potentially any keys that are required for the encryption or secondary PAN derivation process. Thus, this embodiment is particularly useful for conducting secure transactions.

[0077] Embodiments of the invention can have one or more of the following advantages. First, there are no major impacts on the terminal side. Second, routing

is preserved and is not impacted. Third, encryption could be card based or terminal based encryption. Fourth, there are no impacts on the receipt printing and the card holder experience. Fifth, there are no impacts on issuer processing as the issuer is receiving the clear unencrypted data (if the primary PAN is decrypted before it reaches the issuer). Sixth, embodiments of the invention take advantage of preexisting data delivery fields and standard, publicly available and proven encryption methods and algorithms (e.g., the symmetric Triple DES algorithm). Seventh, embodiments of the invention would need only minor system updates on the acquirer side and would use fields that are currently well defined and understood. Eighth, since the data are encrypted, embodiments of the invention can be used against certain counterfeit attacks rendering it difficult to use data obtained at a face to face merchant, mail order, telephone, or Internet based environments. As the data could be encrypted and dynamic, embodiments of the invention can help defend against fraudulent attacks on the merchants' databases as the data is rendered useless.

[0078] 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

[0079] 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.

[0080] The above embodiments described are illustrative and not restrictive. Many variations of the invention will become apparent to those skilled in the art upon review of the disclosure. The scope of the invention should, therefore, be determined not with reference to the described embodiments, but instead should be determined with reference to the accompanying claims.

[0081] One or more features from any embodiment may be combined with one or more features of any other embodiment without departing from the scope of the invention.

[0082] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

THE SUBJECT-MATTER OF THE INVENTION FOR WHICH AN EXCLUSIVE PROPERTY OR PRIVILEGE IS CLAIMED IS DEFINED AS FOLLOWS:

1. A method comprising:

receiving, at a server computer, an authorization request message associated with a transaction, the authorization request message including a secondary PAN associated with a primary PAN, wherein the secondary PAN is within a PAN field of the authorization request message and wherein the primary PAN comprises a primary PAN first end portion and a primary PAN second end portion, and the secondary PAN comprises a secondary PAN first end portion and a secondary PAN second end portion, the secondary PAN second end portion being the same as the primary PAN second end portion;

determining, by the server computer, that the secondary PAN is not a valid primary account number;

based on the determining that the secondary PAN is not valid, obtaining, by the server computer, the primary PAN based upon data at another location outside the PAN field of the authorization request message;

determining, by the server computer based upon the primary PAN, whether the transaction is authorized; and

sending an authorization response message that indicates an approval of the transaction or a disapproval of the transaction.

2. A computer readable medium storing instructions which, when executed by a processor, cause the processor to perform operations comprising:

receiving an authorization request message associated with a transaction, the authorization request message including a secondary PAN associated with a primary PAN, wherein the secondary PAN is within a PAN field of

the authorization request message and wherein the primary PAN comprises a primary PAN first end portion and a primary PAN second end portion, and the secondary PAN comprises a secondary PAN first end portion and a secondary PAN second end portion, the secondary PAN second end portion being the same as the primary PAN second end portion;

determining that the secondary PAN is not a valid primary account number;

based on the determining that the secondary PAN is not valid, obtaining the primary PAN based upon data at another location outside the PAN field of the authorization request message;

determining, based upon the primary PAN, whether the transaction is authorized; and

sending an authorization response message that indicates an approval of the transaction or a disapproval of the transaction.

3. A server computer, comprising:

a processor; and

a computer readable medium storing instructions which, when executed by the processor, cause the server computer to perform operations comprising:

receiving an authorization request message associated with a transaction, the authorization request message including a secondary PAN associated with a primary PAN, wherein the secondary PAN is within a PAN field of the authorization request message and wherein the primary PAN comprises a primary PAN first end portion and a primary PAN second end portion, and the

secondary PAN comprises a secondary PAN first end portion and a secondary PAN second end portion, the secondary PAN second end portion being the same as the primary PAN second end portion;

determining that the secondary PAN is not a valid primary account number;

based on the determining that the secondary PAN is not valid, obtaining the primary PAN based upon data at another location outside the PAN field of the authorization request message;

determining, based upon the primary PAN, whether the transaction is authorized; and

sending an authorization response message that indicates an approval of the transaction or a disapproval of the transaction.

4. The method of claim **1**, wherein:

the primary PAN further comprises a primary PAN middle portion; and

the secondary PAN further comprises a secondary PAN middle portion that is not the same as the primary PAN middle portion, wherein the secondary PAN first end portion is the same as the primary PAN first end portion.

5. The method of claim **4**, wherein the secondary PAN middle portion has a value selected so that a result of a checksum operation performed using a plurality of digits of the secondary PAN matches another result of the checksum operation performed using a corresponding plurality of digits of the primary PAN.

6. The method of claim **5**, wherein:

the result of the checksum operation performed using the plurality of digits of the secondary PAN is a single digit checksum value;

a last digit of the primary PAN second end portion is the single digit checksum value; and

a last digit of the secondary PAN second end portion is the single digit checksum value.

7. The method of claim **4**, wherein the secondary PAN middle portion comprises a plurality of digits, wherein at least a majority of the plurality of digits are identical.

8. The method of claim **7**, wherein all of the plurality of digits except for one of the plurality of digits are identical.

9. The method of claim **7**, wherein all of the plurality of digits are identical.

10. The method of any one of claims **1** and **4-9**, wherein the obtaining the primary PAN based upon the data at the another location outside the PAN field of the authorization request message comprises: decrypting at least some of the data at the another location to yield the primary PAN.

11. The method of any one of claims **1** and **4-10**, wherein the secondary PAN middle portion is based upon a number of times that a portable consumer device has been used by a user.

12. The computer readable medium of claim **2**, wherein:

the primary PAN further comprises a primary PAN middle portion; and

the secondary PAN further comprises a secondary PAN middle portion that is not the same as the primary PAN middle portion, wherein the secondary PAN first end portion is the same as the primary PAN first end portion.

13. The computer readable medium of claim **12**, wherein the secondary PAN middle portion has a value selected so that a result of a checksum operation performed using a plurality of digits of the secondary PAN matches another result of the checksum operation performed using a corresponding plurality of digits of the primary PAN.

14. The computer readable medium of claim **13**, wherein:

the result of the checksum operation performed using the plurality of digits of the secondary PAN is a single digit checksum value;

a last digit of the primary PAN second end portion is the single digit checksum value; and

a last digit of the secondary PAN second end portion is the single digit checksum value.

15. The computer readable medium of claim **12**, wherein the secondary PAN middle portion comprises a plurality of digits, wherein at least a majority of the plurality of digits are identical.

16. The computer readable medium of claim **15**, wherein all of the plurality of digits except for one of the plurality of digits are identical.

17. The computer readable medium of claim **15**, wherein all of the plurality of digits are identical.

18. The computer readable medium of any one of claims **2** and **12-17**, wherein the obtaining the primary PAN based upon the data at the another location outside the PAN field of the authorization request message comprises:

decrypting at least some of the data at the another location to yield the primary PAN.

19. The computer readable medium of any one of claims **2** and **12-18**, wherein the secondary PAN middle portion is based upon a number of times that a portable consumer device has been used by a user.

20. The server computer of claim **3**, wherein:

the primary PAN further comprises a primary PAN middle portion; and

the secondary PAN further comprises a secondary PAN middle portion that is not the same as the primary PAN middle portion, wherein the secondary PAN first end portion is the same as the primary PAN first end portion.

21. The server computer of claim **20**, wherein the secondary PAN middle portion has a value selected so that a result of a checksum operation performed using a plurality of digits of the secondary PAN matches another result of the checksum operation performed using a corresponding plurality of digits of the primary PAN.

22. The server computer of claim **21**, wherein:

the result of the checksum operation performed using the plurality of digits of the secondary PAN is a single digit checksum value;

a last digit of the primary PAN second end portion is the single digit checksum value; and

a last digit of the secondary PAN second end portion is the single digit checksum value.

23. The server computer of claim **20**, wherein the secondary PAN middle portion comprises a plurality of digits, wherein at least a majority of the plurality of digits are identical.

24. The server computer of claim **23**, wherein all of the plurality of digits except for one of the plurality of digits are identical.

25. The server computer of claim **23**, wherein all of the plurality of digits are identical.

26. The server computer of any one of claims **3** and **20-25**, wherein the obtaining the primary PAN based upon the data at the another location outside the PAN field of the authorization request message comprises:

decrypting at least some of the data at the another location to yield the primary PAN.

27. The server computer of any one of claims **3** and **20-26**, wherein the secondary PAN middle portion is based upon a number of times that a portable consumer device has been used by a user.

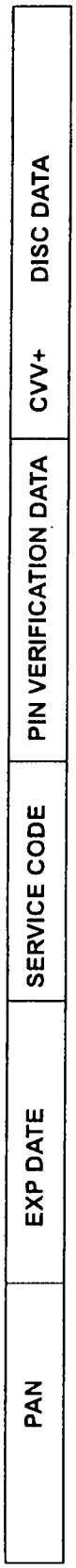

FIG. 1

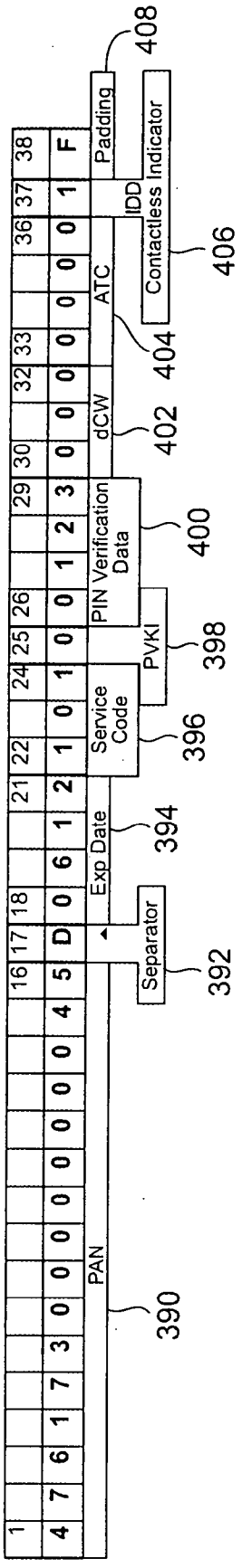

FIG. 2

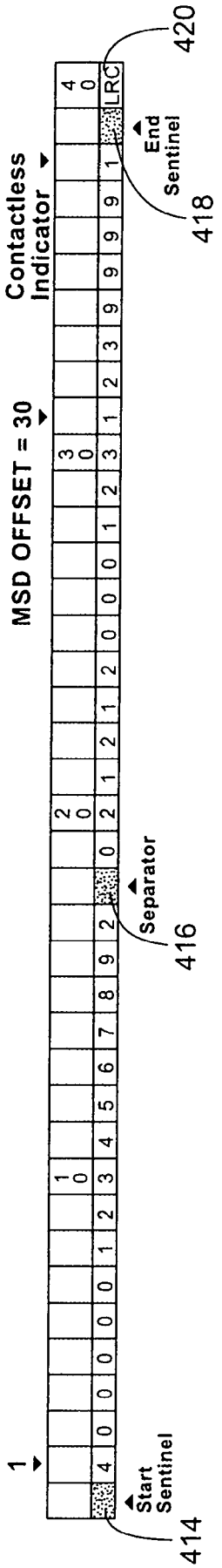

FIG. 3

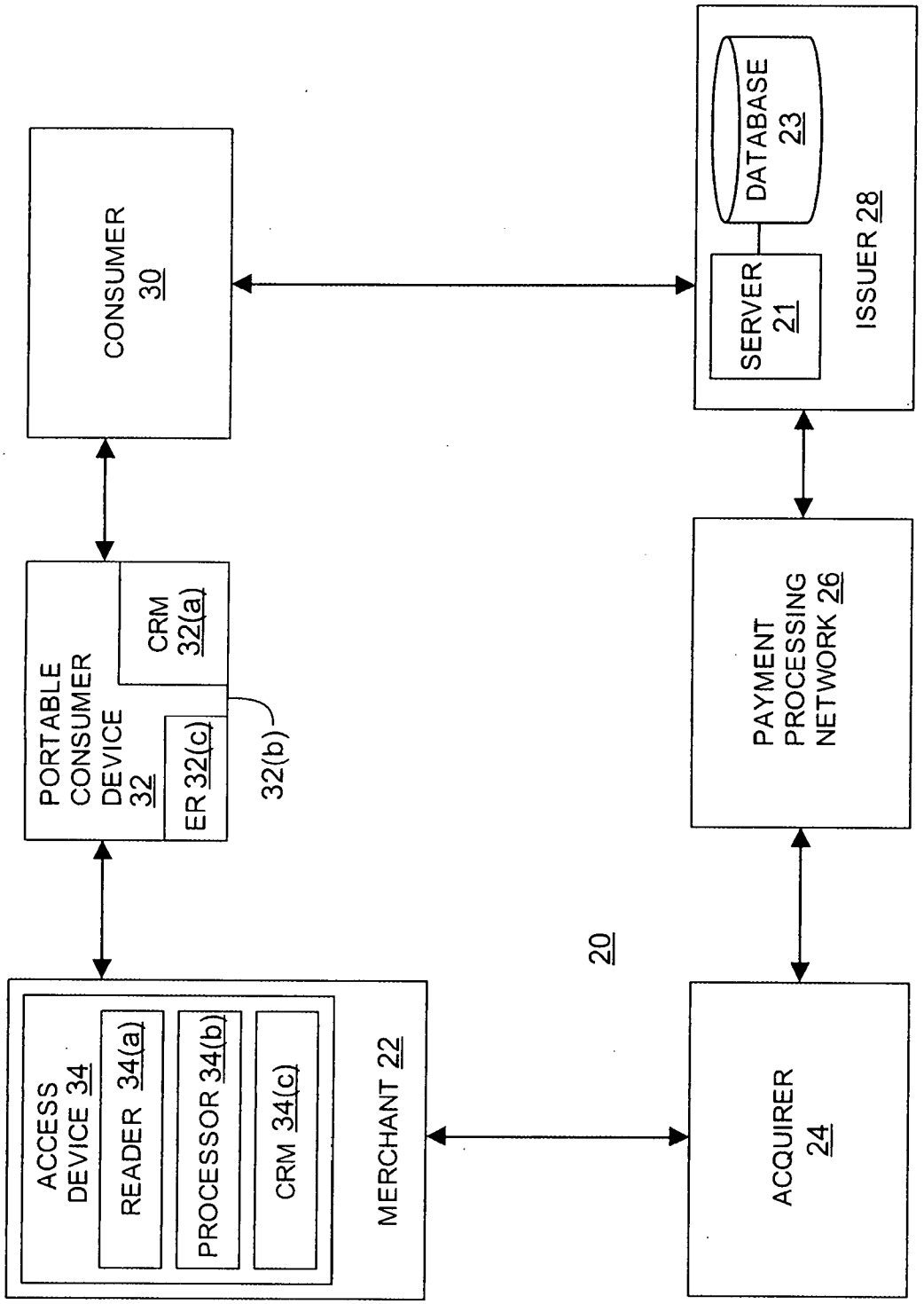
CONSUMER 30
ISSUER 28
DATABASE 23
SERVER 21
PORTABLE CONSUMER DEVICE 32
CRM 32(a)
ER 32(c)
32(b)
PAYMENT PROCESSING NETWORK 26
20
ACCESS DEVICE 34
READER 34(a)
PROCESSOR 34(b)
CRM 34(c)
MERCHANT 22
ACQUIRER 24

FIG. 4

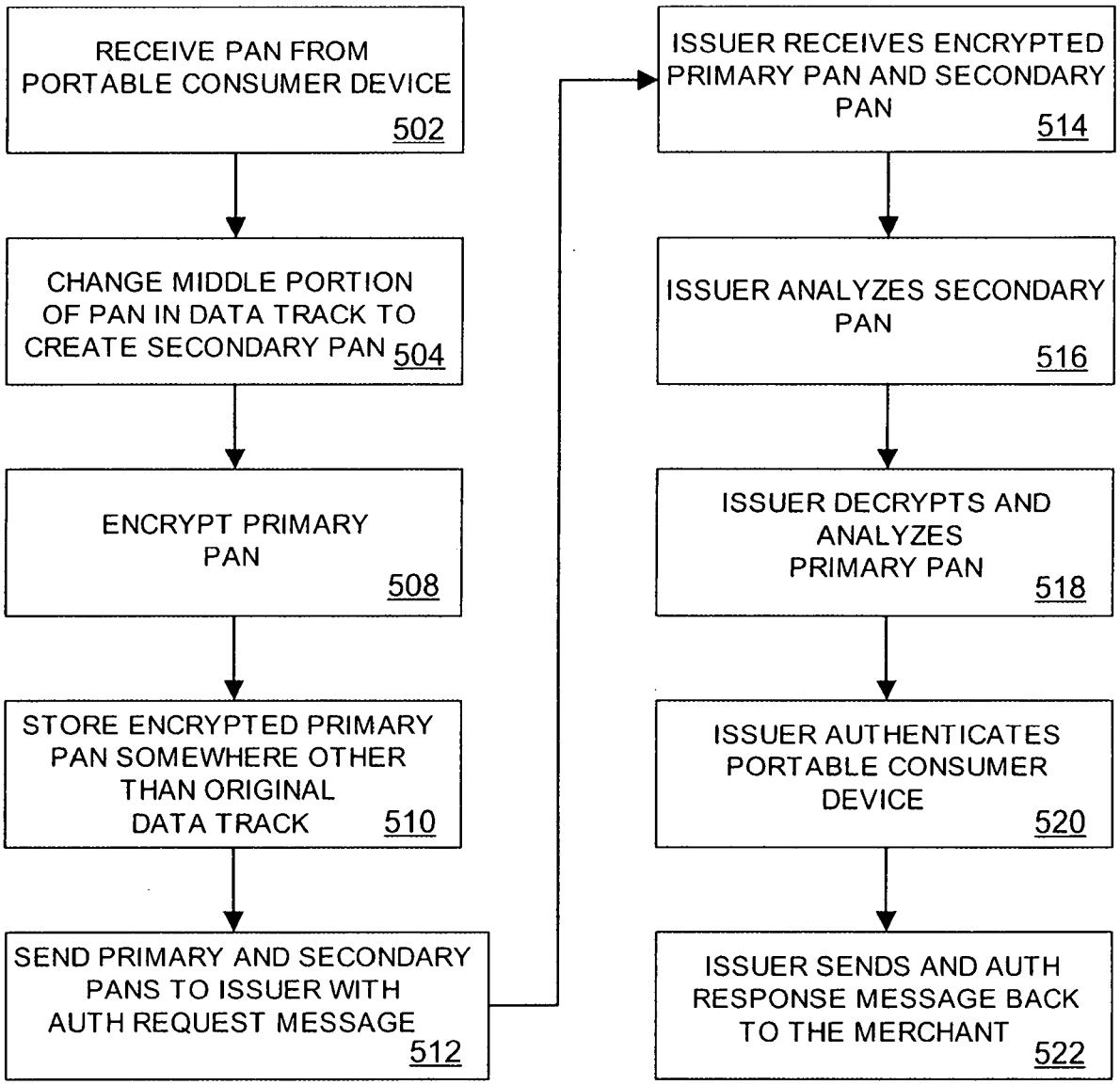
RECEIVE PAN FROM PORTABLE CONSUMER DEVICE 502
CHANGE MIDDLE PORTION OF PAN IN DATA TRACK TO CREATE SECONDARY PAN 504
ENCRYPT PRIMARY PAN 508
STORE ENCRYPTED PRIMARY PAN SOMEWHERE OTHER THAN ORIGINAL DATA TRACK 510
SEND PRIMARY AND SECONDARY PANS TO ISSUER WITH AUTH REQUEST MESSAGE 512
ISSUER RECEIVES ENCRYPTED PRIMARY PAN AND SECONDARY PAN 514
ISSUER ANALYZES SECONDARY PAN 516
ISSUER DECRYPTS AND ANALYZES PRIMARY PAN 518
ISSUER AUTHENTICATES PORTABLE CONSUMER DEVICE 520
ISSUER SENDS AND AUTH RESPONSE MESSAGE BACK TO THE MERCHANT 522

FIG. 5

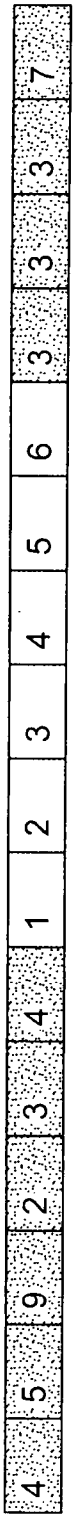

FIG. 6(a)

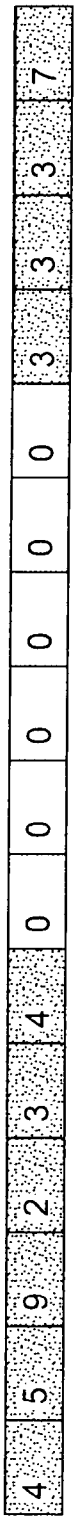

FIG. 6(b)

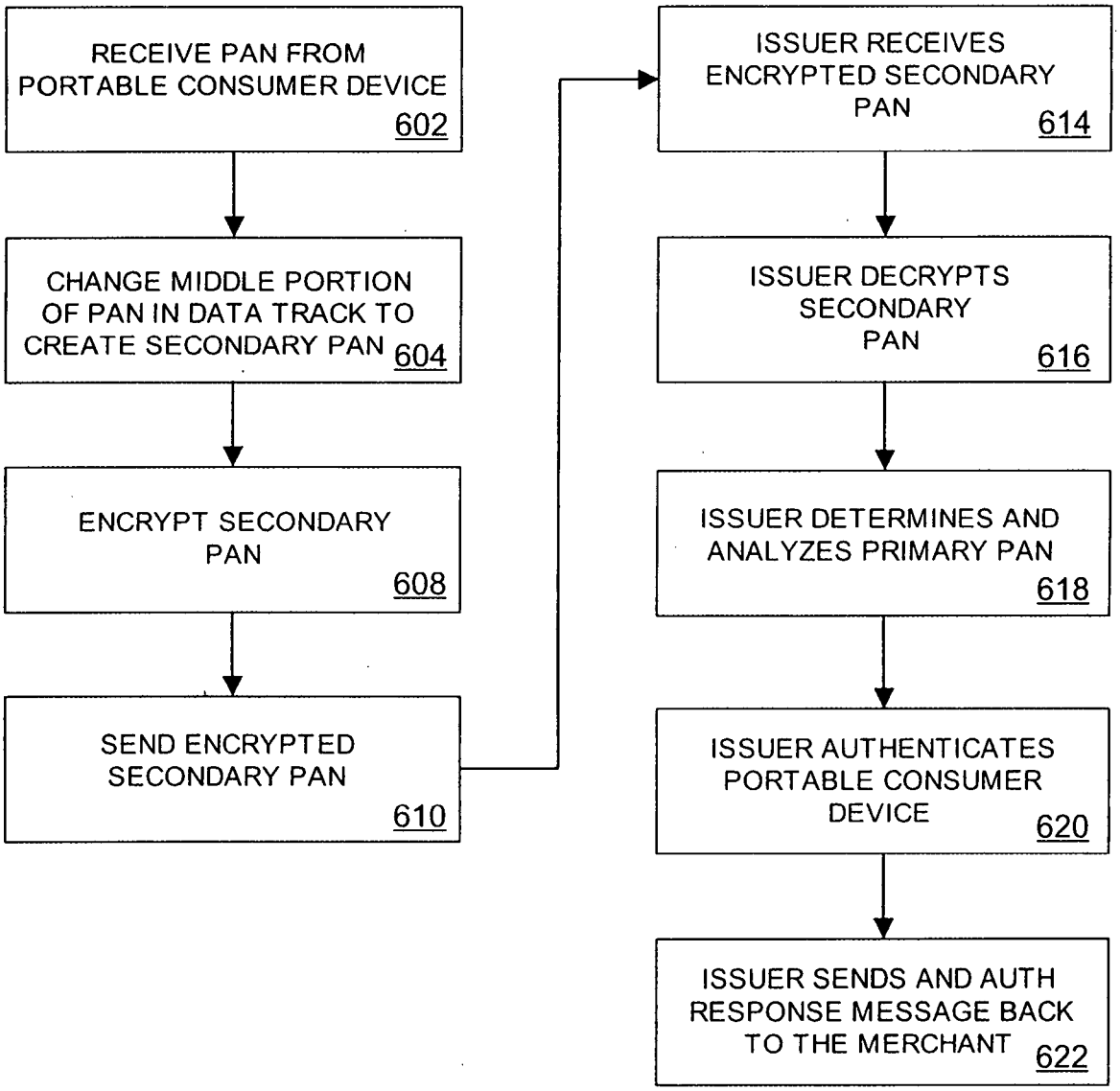
RECEIVE PAN FROM PORTABLE CONSUMER DEVICE 602
CHANGE MIDDLE PORTION OF PAN IN DATA TRACK TO CREATE SECONDARY PAN 604
ENCRYPT SECONDARY PAN 608
SEND ENCRYPTED SECONDARY PAN 610
ISSUER RECEIVES ENCRYPTED SECONDARY PAN 614
ISSUER DECRYPTS SECONDARY PAN 616
ISSUER DETERMINES AND ANALYZES PRIMARY PAN 618
ISSUER AUTHENTICATES PORTABLE CONSUMER DEVICE 620
ISSUER SENDS AND AUTH RESPONSE MESSAGE BACK TO THE MERCHANT 622

FIG. 7

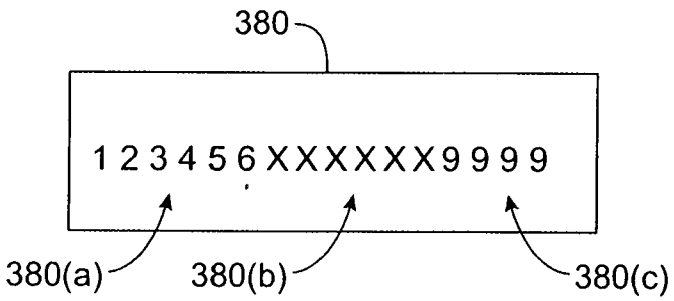

FIG. 8


PAN
EXP DATE
SERVICE CODE
PIN VERIFICATION DATA
CVV+
DISC DATA