



US 20190197552A1

(19) **United States**(12) **Patent Application Publication**
Kumnick et al.(10) **Pub. No.: US 2019/0197552 A1**(43) **Pub. Date: Jun. 27, 2019**(54) **PAYMENT ACCOUNT IDENTIFIER SYSTEM**

continuation of application No. 14/597,072, filed on Jan. 14, 2015, now Pat. No. 9,846,878.

(71) Applicant: **Visa International Service Association**, San Francisco, CA (US)

(60) Provisional application No. 61/927,381, filed on Jan. 14, 2014.

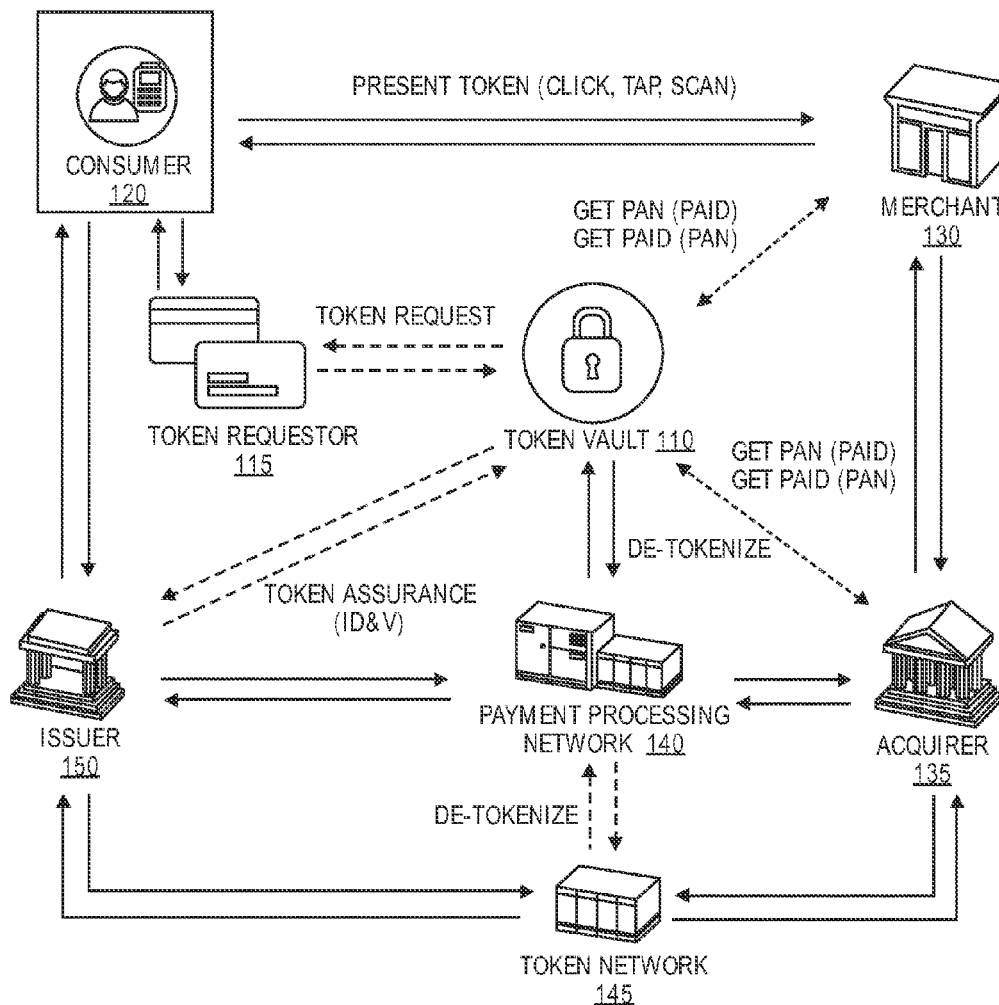
(72) Inventors: **Phillip Kumnick**, Phoenix, AZ (US);
Joseph Bjorn Ovick, San Francisco, CA (US); **Chandra Srivastava**, San Jose, CA (US)**Publication Classification**(51) **Int. Cl.****G06Q 20/40** (2006.01)**G06Q 20/36** (2006.01)(52) **U.S. Cl.**CPC **G06Q 20/4016** (2013.01); **G06Q 20/3674** (2013.01)(21) Appl. No.: **16/293,488**(22) Filed: **Mar. 5, 2019****Related U.S. Application Data**

(63) Continuation of application No. 16/052,354, filed on Aug. 1, 2018, now Pat. No. 10,269,018, which is a continuation of application No. 15/814,994, filed on Nov. 16, 2017, now Pat. No. 10,062,079, which is a

(57)

ABSTRACT

A method for utilizing a non-transactable account identifier with a payment token is disclosed. The non-transactable account identifier can have the same format as a primary account number (PAN) and the payment token, but is not used to conduct a payment transaction.



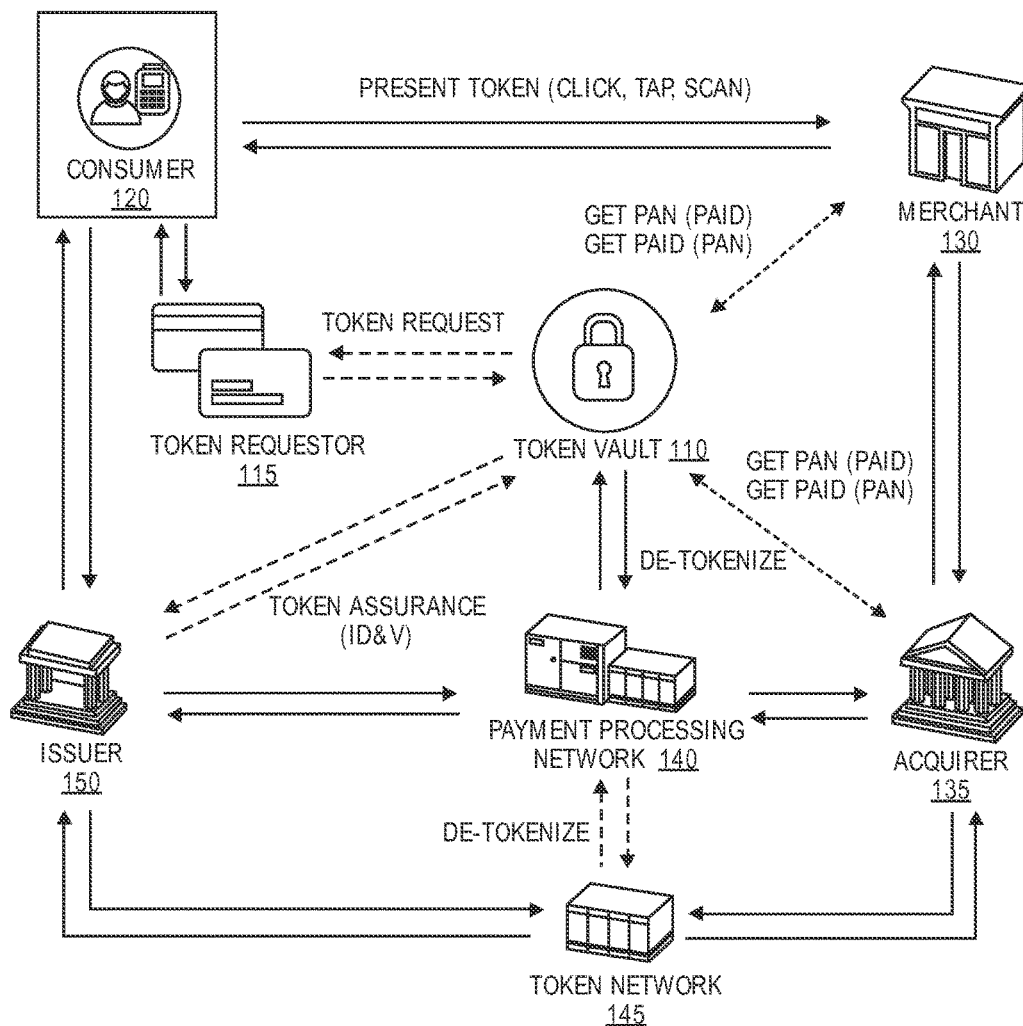
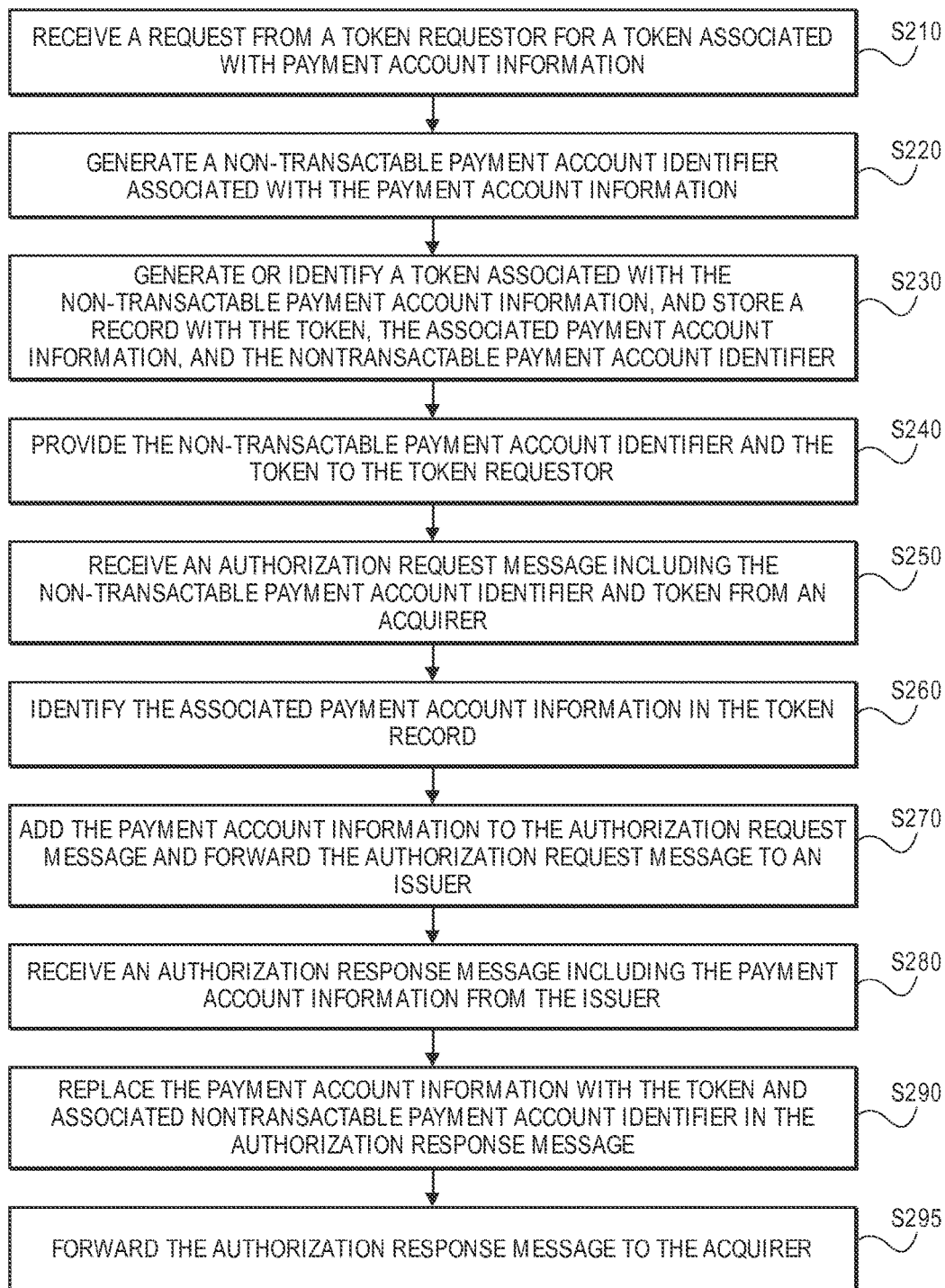
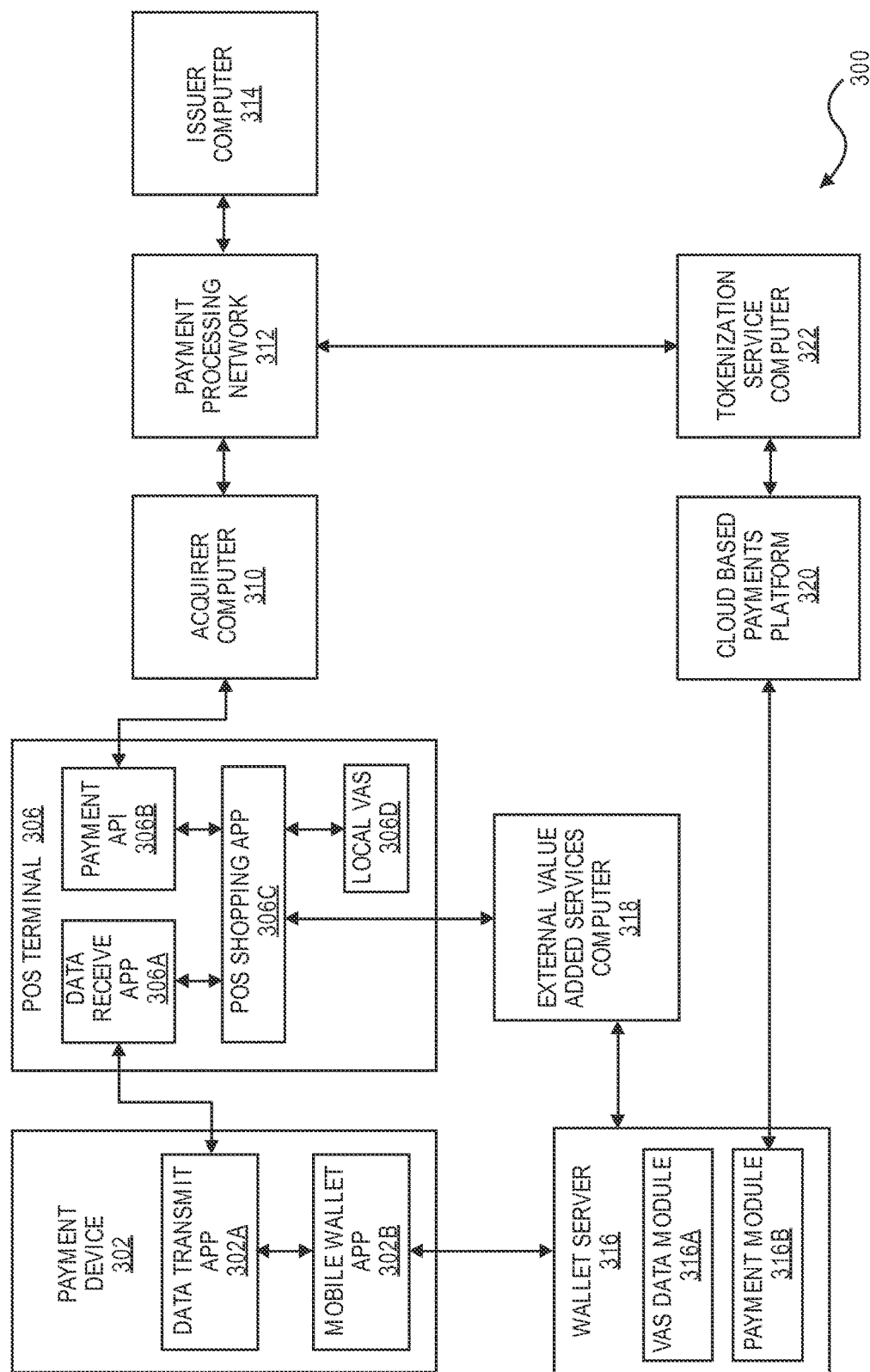


FIG. 1

**FIG. 2**



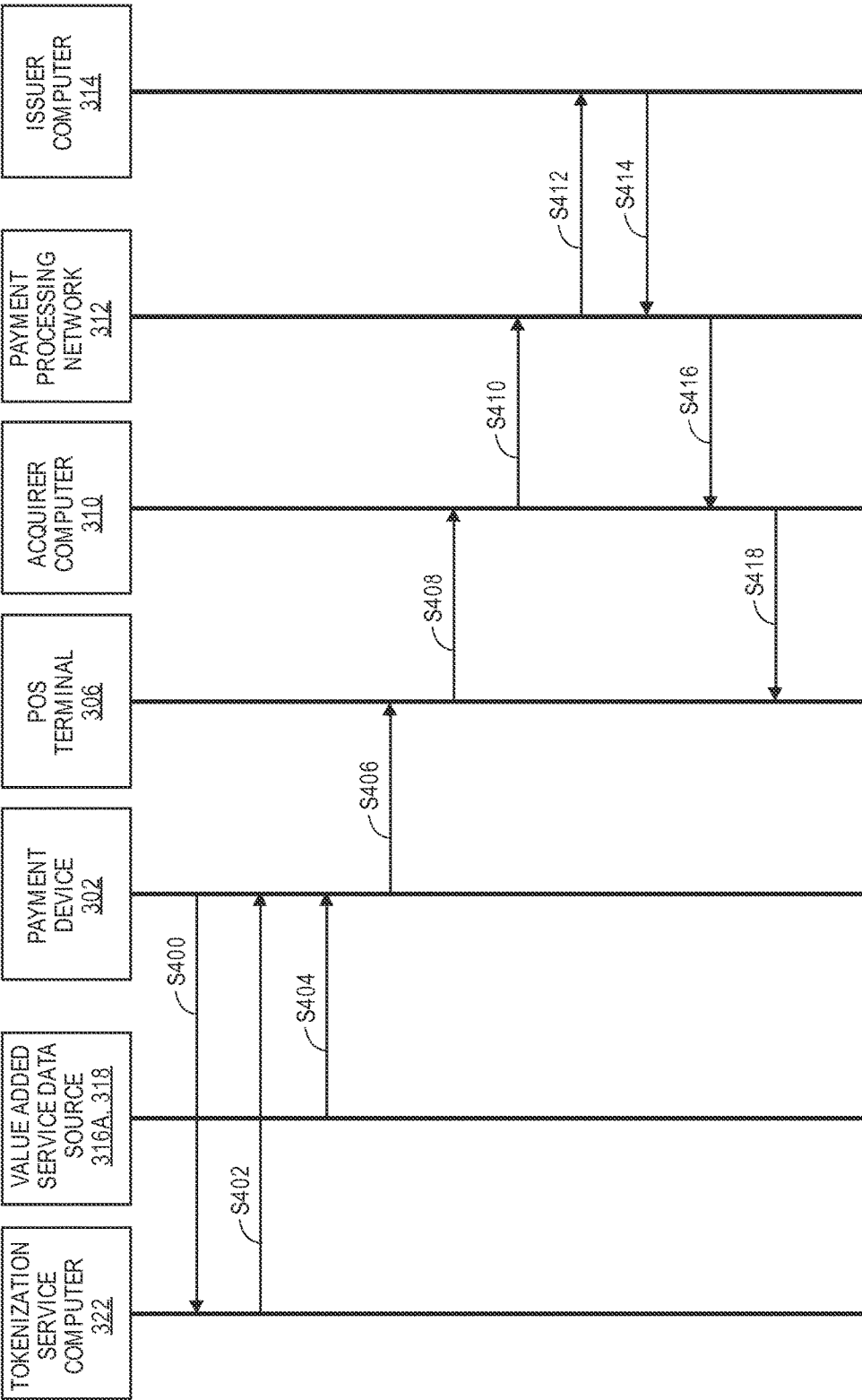


FIG. 4

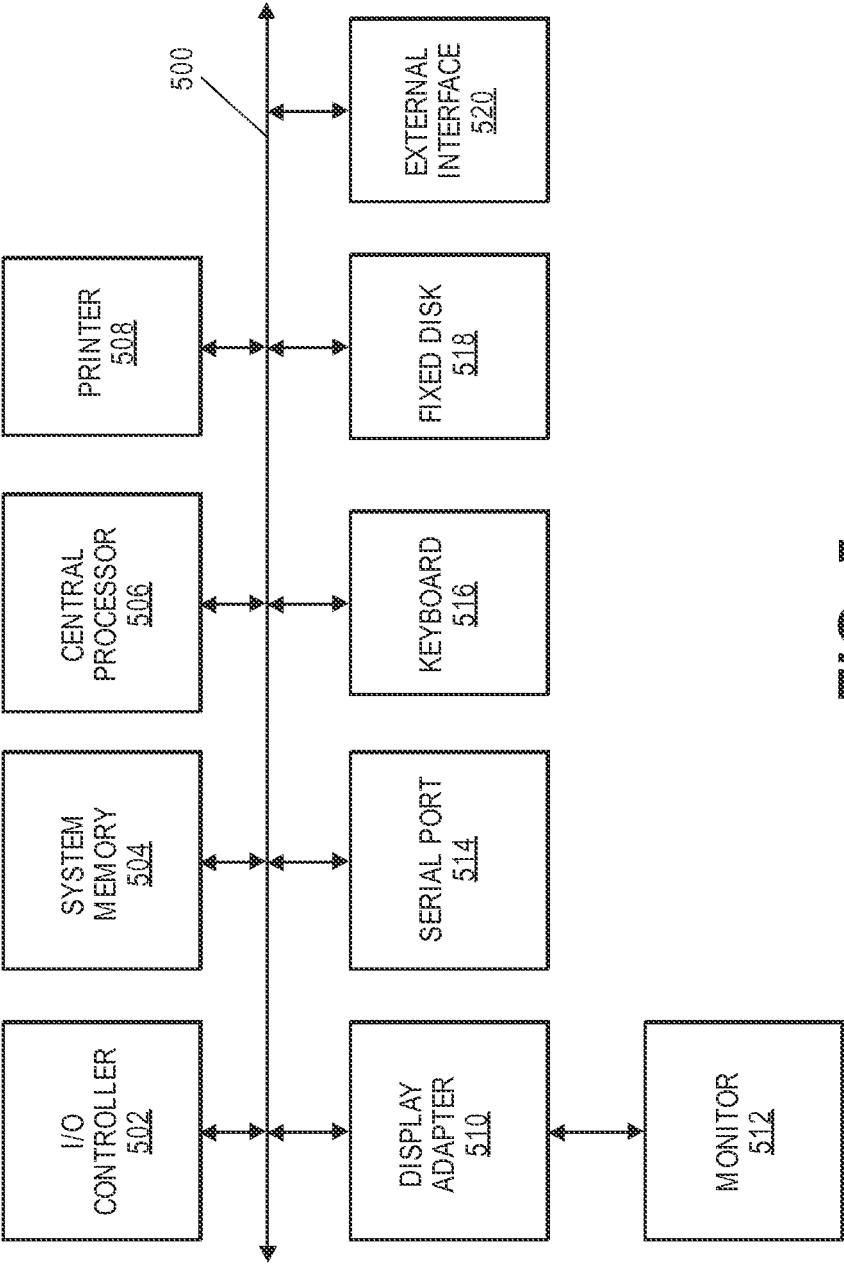


FIG. 5

PAYMENT ACCOUNT IDENTIFIER SYSTEM

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application is a non-provisional application of and claims the benefit of the filing date of U.S. Provisional Application No. 61/927,381, filed on Jan. 14, 2014, which is herein incorporated by reference in its entirety for all purposes.

BACKGROUND

[0002] In the current payments ecosystem, merchants, processors and acquirers currently use PANs (primary account numbers) to process payment transactions and to identify cardholders for loyalty programs, fraud checks and reporting.

[0003] While the use of PANs for such purposes has been useful, the use of PANs as accountholder identification mechanisms is problematic. If PANs are retained by merchants, for example, the merchants will need to be PCI (payment card industry) compliant. To be PCI compliant, merchants need to take a number of steps to improve the security of their data systems. Such steps can be resource and time intensive to implement and maintain.

[0004] One way to avoid the need to be PCI compliant is to use payment tokens or “tokens” instead of PANs. Tokens can be substitutes for real PANs. A token can be used in place of a real PAN in a payment transaction. If the token is stolen by an unauthorized user (e.g., a hacker), then a new token can be issued in place of the token that was stolen. In this situation, the underlying real PAN is protected and the consumer’s basic account information need not be re-issued.

[0005] Although the use of tokens is desirable, the number of tokens used in a particular payments ecosystem can be very large. In some cases, each accountholder PAN can be mapped to multiple tokens (1-N mapping). For example, if a PAN is used in multiple digital wallets, each wallet instance can have a different static token for the same cardholder PAN. In another example, a different token relating to a PAN can be issued for each transaction.

[0006] Because the number of tokens corresponding to a single PAN is unknown to an entity such as merchant, and because a token is intended to obscure a real PAN, it is difficult if not impossible for an entity such as a merchant to determine who the accountholder is if the merchant is in possession of the token. As such, in a conventional token based payments system, entities such as merchants are unable to perform fraud processing, operate loyalty programs, and other processes that would necessarily require them to know who the accountholder is or might be.

[0007] Embodiments of the invention address these and other problems, individually and collectively.

SUMMARY

[0008] Embodiments of the invention can relate to systems and methods that can utilize payment tokens and non-transactable payment account identifiers. In some embodiments of the invention, a non-transactable payment account identifier may have the same format as a PAN. Because of this, an entity’s existing processing system (i.e., systems that process PANs) can utilize the non-transactable payment account identifier much like it would for a real PAN. However, unlike a PAN or a transactable payment token, the

non-transactable payment account identifier cannot be used to conduct a payment transaction. Consequently, the non-transactable payment account identifiers according to embodiments of the invention can be stored and used by entities such as merchants, acquirers, and program operators to perform operations including loyalty processing, fraud processing, and reporting, even though tokens are used to conduct payment transactions. As such, such entities do not need to be PCI compliant.

[0009] One embodiment of the invention is directed to a method. The method comprises receiving, by a token service computer, a token request comprising a primary account identifier from a token requestor computer, and then determining, by the token service computer, a transactable payment token and a non-transactable payment account identifier associated with the primary account identifier. The method also includes transmitting, by the token service computer, the transactable payment token and the non-transactable payment account identifier to the token requestor computer. If the token requestor computer is not a consumer’s payment device, the token requestor computer may provide the transactable payment token and the non-transactable payment account identifier to the payment device. The transactable payment token and the non-transactable payment account identifier can then be passed from the consumer’s payment device to an access device to conduct a transaction. The transactable payment token can be used by the access device to process a payment for the transaction instead of the primary account identifier, while the non-transactable payment account identifier can be used as a reference for the primary account identifier to perform an operation that is not a payment transaction.

[0010] Another embodiment of the invention is directed to a token service computer configured to perform the above-described method.

[0011] Another embodiment of the invention is directed to a method comprising receiving, by a token service system, a token request associated with account information and then determining a non-transactable payment account identifier and a payment token. The method also includes providing the non-transactable payment account identifier and a token associated with the account information, and then receiving an authorization request message including the token and the non-transactable payment account identifier from a merchant. The method also includes adding the account information to the authorization request message and sending the authorization request message to an issuer. The method further includes receiving an authorization response message including the account information from the issuer and replacing the account information with the transactable payment token and the non-transactable payment account identifier in the authorization response message. The method further includes sending the authorization response message to the merchant.

[0012] Another embodiment of the invention is directed to a token service system configured to perform the above-described method.

[0013] Further details regarding embodiments of the invention can be found in the Detailed Description and the Figures.

BRIEF DESCRIPTION OF THE DRAWINGS

[0014] FIG. 1 shows a block diagram of a system according to an embodiment of the invention.

[0015] FIG. 2 shows a flowchart illustrating a method according to an embodiment of the invention.

[0016] FIG. 3 shows a block diagram of another system according to an embodiment of the invention.

[0017] FIG. 4 shows a flow diagram illustrating methods that can be used with the system illustrated in FIG. 3.

[0018] FIG. 5 shows a block diagram of a computer apparatus according to an embodiment of the invention.

DETAILED DESCRIPTION

[0019] Embodiments of the invention use a non-transactable payment account identifier to allow entities (e.g., merchant, acquirer, etc.) within a transaction eco-system to identify an accountholder when using tokens in lieu of traditional PANs. The non-transactable payment account identifier enables entities such as merchants and acquirers to identify accountholders when using transactable payment tokens for various applications. Such applications include, but are not limited to: fraud and risk checks on transaction authorization requests, fraud and risk reviews after transactions are completed, performance of value added services (e.g., loyalty, backend applications, reporting), and transaction feeds for third party value added applications.

[0020] Prior to discussing specific embodiments of the invention, some terms may be described in detail.

[0021] A “non-transactable payment account identifier” (alternatively referred to as a “PAID”) may be any string of characters that identify an accountholder and that is not used to conduct a payment transaction on an underlying account. For example, in some embodiments, a non-transactable payment account identifier may be 16-19 digits (or any other suitable length) and may be based on the format and rules of a PAN (primary account number). The non-transactable payment account identifier may be static over time and any number of transactions. A non-transactable account identifier may have a BIN (bank identification number) that is the same as the BIN for the corresponding real account identifier. Alternatively, it may have a BIN that is derived from or completely random with respect to the real BIN. The BIN in the non-transactable account identifier could also be a static tokenized BIN.

[0022] In some embodiments, the non-transactable payment account identifier may include one or more characters that may indicate that it cannot be used to conduct a payment transaction. For example, it could be that all non-transactable payment account identifiers may start with the characters “99.” Any data strings that are similar in length to a real PAN in any transaction request messages would be treated by any suitable payment processing computers as being non-transactable. In other embodiments, non-transactable payment account identifiers may not be readily identified as being non-transactable by an outside observer. For example, a token service computer (e.g., a token vault) may generate a list of non-transactable payment account identifiers, and that list may be distributed by the token service computer to any entity (e.g., a merchant) that may wish to store or use the non-transactable payment account identifiers. If one tries to use the non-transactable payment account identifier to conduct a transaction, it will not be processed and/or routed by one or more computers in the payments system.

[0023] “Payment account information” may be any information that identifies or is associated with a payment account. Payment account information may be provided in

order to make a payment from a payment account. Some examples of payment account information include one or more of a PAN (primary account number), a CVV (card verification value), a dCVV (dynamic card verification value), a user name, an expiration date, a gift card number or code, etc.

[0024] A “real account identifier” may include a transactable identifier associated with a payment account that directly represents the payment account. For example, a real account identifier may be a primary account number (PAN) issued by an issuer for a card account (e.g., credit card, debit card, etc.). For instance, in some embodiments, a real account identifier may include a sixteen digit numerical value such as “4147 0900 0000 1234.” The first six digits of the real account identifier (e.g., “414709”), may represent a real issuer identifier (e.g., a “BIN” or bank identification number) that may identify an issuer associated with the real account identifier.

[0025] “Tokenization” is a process by which data is replaced with substitute data. For example, a payment account identifier (e.g., a primary account number (PAN)) may be tokenized by replacing the primary account identifier with a substitute number (e.g. a token) that may be associated with the payment account identifier. Further, tokenization may be applied to any other-information which may be replaced with a substitute value (i.e., token). Tokenization may be used to enhance transaction efficiency, improve transaction security, increase service transparency, or to provide a method for third-party enablement.

[0026] “Token exchange” or “de-tokenization” can include a process of restoring the data that was substituted during tokenization. For example, a token exchange may include replacing a payment token with a corresponding primary account number (PAN) that was associated with the payment token during tokenization of the PAN. Thus, the de-tokenization may refer to the process of redeeming a token for the associated PAN value based on a token-to-PAN mapping stored, for example, in a token vault. The ability to retrieve a PAN in exchange for the associated token may be restricted to specifically authorized entities, individuals, applications, or systems. Further, de-tokenization or token exchange may be applied to any other information. In some embodiments, token exchange may be achieved via a transactional message, such as an ISO message, an application programming interface (API), or another type of web interface (e.g., web request).

[0027] A “transactable payment token” may include an identifier for a payment account that is a substitute for an account identifier, such as a primary account number (PAN). For example, a token may include a series of alphanumeric characters that may be used as a substitute for an original account identifier. For example, a token “4900 0000 0000 0001” may be used in place of a PAN “4147 0900 0000 1234.” In some embodiments, a token may be “format preserving” and may have a numeric format that conforms to the account identifiers used in existing payment processing networks (e.g., ISO 8583 financial transaction message format). In some embodiments, a token may be used in place of a PAN to initiate, authorize, settle or resolve a payment transaction or represent the original credential in other systems where the original credential would typically be provided. In some embodiments, a token value may be generated such that the recovery of the original PAN or other account identifier from the token value may not be compu-

tationally derived. Further, in some embodiments, the token format may be configured to allow the entity receiving the token to identify it as a token and recognize the entity that issued the token.

[0028] A “Bank Identification Number (BIN)” may be a number that identifies a bank. A BIN may be assigned by a payment network to an issuer of a payment account. BINs may be consistent with industry account and issuer identification specifications (e.g. ISO 7812) such that the payment network assigning the BIN may be identified based on the BIN and associated account ranges.

[0029] A “token BIN” may refer to a specific BIN that has been designated only for the purpose of issuing tokens and may be flagged accordingly in BIN tables. Token BINs may not have a dual purpose and may not be used to issue both primary account numbers (PANs) and tokens.

[0030] A “token issuer identifier range (issuer BIN range)” may refer to a unique identifier (e.g., of 6 to 12 digits length) originating from a set of pre-allocated token issuer identifiers (e.g., 6 digit token BINs). For example, in some embodiments, one or more token BIN ranges can be allocated to each issuer BIN range that is associated with an issuer. In some embodiments, the token BIN ranges may be used to generate a payment token and may not be used to generate a non-payment token. In some embodiments, a token may pass the basic validation rules of an account number including, for example, a LUHN check or checksum validation that may be set up by different entities within the payment system. In some embodiments, a payment token issuer identifier may be mapped to a real issuer identifier (e.g., a BIN) for an issuer. For example, a payment token issuer identifier may include a six digit numerical value that may be associated with an issuer. For instance, any token including the payment token issuer identifier may be associated with a particular issuer. As such, the issuer may be identified using the corresponding issuer identifier range associated with the token issuer identifier. For example, a payment token issuer identifier “490000” corresponding to a payment token “4900 0000 0000 0001” can be mapped to an issuer identifier “414709” corresponding to a payment account identifier “4147 0900 0000 1234”. In some embodiments, a payment token issuer identifier is static for an issuer. For example, a payment token issuer identifier (e.g., “490000”) may correspond to a first issuer and another payment token issuer identifier (e.g., “520000”) may correspond to a second issuer, and the first and second payment token issuer identifiers may not be changed or altered without informing all entities within the network token processing system. In some embodiments, a payment token issuer identifier range may correspond to an issuer identifier. For example, payment tokens including payment token issuer identifiers from “490000”-“490002” may correspond to a first issuer (e.g., mapped to issuer identifier “414709”) and payment tokens including payment token issuer identifiers from “520000”-“520002” may correspond to a second issuer (e.g., mapped to real issuer identifier “417548”). Token BIN Ranges and assignment of tokens from these BIN ranges may be made available to the parties (e.g., via routing tables) accepting the transaction to make routing decisions.

[0031] A “token service system” can include a system that that services payment tokens. In some embodiments, a token service system can facilitate requesting, determining (e.g., generating) and/or issuing tokens, as well as maintaining an

established mapping of tokens to primary account numbers (PANs) in a repository (e.g. token vault). In some embodiments, the token service system may establish a token assurance level for a given token to indicate the confidence level of the token to PAN binding. The token service system may support token processing of payment transactions submitted using tokens by de-tokenizing the token to obtain the actual PAN. In some embodiments, a token service system may include a token service computer alone, or in combination with other computers such as a payment processing network computer.

[0032] A “token service provider” may include an entity that services payment tokens. In some embodiments, the token service provider may operate one or more server computers in a token service system that generate, process and maintain tokens. The token service provider may include or be in communication with a token vault where the generated tokens are stored. Specifically, the token vault may maintain one-to-one mapping between a token and a primary account number (PAN) represented by the token. The token service provider may have the ability to set aside licensed BINs as token BINs to issue tokens for the PANs that may be submitted to the token service provider. Various entities of a tokenization ecosystem may assume the roles of the token service provider. For example, payment networks and issuers or their agents may become the token service provider by implementing the token services according to embodiments of the present invention. A token service provider may provide reports or data output to reporting tools regarding approved, pending, or declined token requests, including any assigned token requestor IDs. The token service provider may provide data output related to token-based transactions to reporting tools and applications and present the token and/or PAN as appropriate in the reporting output.

[0033] A “token vault” may be an example of a token service computer and can include a repository that maintains established token-to-PAN mappings. According to various embodiments, the token vault may also maintain other attributes of the token requestor that may be determined at the time of registration. The attributes may be used by the token service provider to apply domain restrictions or other controls during transaction processing. In some embodiments, the token vault may be a part of the token service system or the token service provider. Alternatively, the token vault may be a remote repository accessible to the token service provider. Token vaults, due to the sensitive nature of the data mappings that are stored and managed in them, may be protected by strong underlying physical and logical security.

[0034] An “identification and verification (ID&V) method” may be used to evaluate whether the person conducting the transaction is the legitimate account holder. Examples of ID&V methods may include, but are not limited to, an account verification message, a risk score based on assessment of the primary account number (PAN) and use of one time password by the issuer or its agent to verify the account holder. Exemplary ID&V methods may be performed using information such as a user signature, a password, an offline or online personal identification number (PIN), an offline or online enciphered PIN, a combination of offline PIN and signature, a combination of offline enciphered PIN and signature, user biometrics (e.g. voice recognition, fingerprint matching, etc.), a pattern, a glyph,

knowledge-based challenge-responses, hardware tokens (multiple solution options), one time passwords (OTPs) with limited use, software tokens, two-channel authentication processes (e.g., via phone), etc. Using the ID&V, a confidence level may be established with respect to the token to PAN binding.

[0035] A “token assurance level” may include an indicator or a value that allows the token service provider to indicate the confidence level of the token to PAN binding. The token assurance level may be determined by the token service provider based on the type of identification and verification (ID&V) performed and the entity that performed the ID&V. The token assurance level may be set when issuing the token. The token assurance level may be updated if additional ID&V is performed.

[0036] A “requested token assurance level” may include a token assurance level requested by the token requestor. The requested token assurance level may be included in a field of a token request message sent by the requestor to the token service provider for the generation/issuance of the token.

[0037] An “assigned token assurance level” may include an actual (i.e. generated) value assigned by the token service provider to the token as the result of the identification and verification (ID&V) process performed by an entity within the tokenization ecosystem. The assigned token assurance level may be provided back to the token requestor in response to the token request message. The assigned token assurance level may be different than the requested token assurance level included in the token request message.

[0038] “Token attributes” may include any feature or information about a token. For example, token attributes may include information that can determine how a token can be used, delivered, issued, or otherwise how data may be manipulated within a transaction system. For example, the token attributes may include a type of token, frequency of use, token expiry date and/or expiry time, a number of associated tokens, a transaction lifecycle expiry date, and any additional information that may be relevant to any entity within a tokenization ecosystem. For example, token attributes may include a wallet identifier associated with the token, an additional account alias or other user account identifier (e.g., an email address, username, etc.), a device identifier, an invoice number, etc. In some embodiments, a token requestor may provide token attributes at the time of requesting the generation of tokens. In some embodiments, a network token system, payment network associated with the network token system, an issuer, or any other entity associated with the token may determine and/or provide the token attributes associated with a particular token.

[0039] A “token presentment mode” may indicate a method through which a token is submitted for a transaction. Some non-limiting examples of the token presentment mode may include machine readable codes (e.g., quick response code (QRC), barcode, etc.), mobile contactless modes (e.g., near-field communication (NFC) communication), e-commerce remote modes, e-commerce proximity modes, and any other suitable modes in which to submit a token. Tokens may be provided through any number of different methods. For example, in one implementation, a token may be embedded in machine-readable code which may be generated by a wallet provider, mobile application, or other application on mobile device and displayed on a display of the mobile device. The machine readable code can be scanned at the POS through which the token is passed to the merchant. A

mobile contactless mode may include passing the token through NFC in a contactless message. An e-commerce remote mode may include submitting a token by a consumer or a wallet provider through an online transaction or as an e-commerce transaction using a merchant application or other mobile application. An e-commerce proximity mode may include submitting a token by a consumer from a wallet application on a mobile device at a merchant location.

[0040] A “token requestor” include an entity that requests a token. The token requestor may initiate a request that a primary account number (PAN) be tokenized by submitting a token request message to the token service provider. According to various embodiments, a token requestor may no longer need to store a PAN associated with a token once the requestor has received a requested token. The requestor may be an application, a device, a process, or a system that is configured to perform actions associated with tokens. A token requestor can request registration with a network token system, request token generation, token activation, token de-activation, token exchange, token lifecycle management related processes, and/or any other token related processes. A requestor may interface with a network token system through any suitable communication networks and/or protocols (e.g., using HTTPS, SOAP and/or an XML interface among others). Some non-limiting examples of token requestors may include, for example, communication devices (e.g., mobile phones and computers) operated by consumers, card-on-file merchants, acquirers, acquirer processors, and payment gateways acting on behalf of merchants, payment enablers (e.g., original equipment manufacturers, mobile network operators, etc.), digital wallet providers, issuers, third party wallet providers, and/or payment processing networks. In some embodiments, a token requestor can request tokens for multiple domains and/or channels. A token requestor may be registered and identified uniquely by the token service provider within the tokenization ecosystem. During token requestor registration, the token service provider may formally process the token requestor’s application to participate in the token service system. The token service provider may collect information pertaining to the nature of the requestor and the relevant use of tokens to validate and formally approve the token requestor and establish appropriate domain restriction controls. Successfully registered token requestors may be assigned a token requestor identifier that may also be entered and maintained within the token vault. Token requestors be revoked or assigned new token requestor identifiers. This information may be subject to reporting and audit by the token service provider.

[0041] A “token requestor identifier (ID)” may include an identifier for a token requestor. It may include any characters, numerals, or other identifiers associated with an entity associated with a network token system. In some embodiments, a unique token requestor ID may be assigned for each domain for a token request associated with the same token requestor. For example, a token requestor ID can identify a pairing of a token requestor (e.g., a mobile device, a mobile wallet provider, etc.) with a token domain (e.g., e-commerce, contactless, etc.). A token requestor ID may include any format or type of information. For example, in one embodiment, the token requestor ID may include an alpha-numerical value such as a ten digit or an eleven digit letter and/or number (e.g., 4678012345). In some embodiments, a token requestor ID may include a code for a token service

provider (e.g., first 3 digits) such as the network token system and the remaining digits may be assigned by the token service provider for each requesting entity (e.g., mobile wallet provider) and the token domain (e.g., contactless, e-commerce, etc.).

[0042] A “token request indicator” may refer to an indicator used to indicate that a message is related to a token request. The token request indicator may optionally be passed to the issuer as part of the Identification and Verification (ID&V) method to inform the issuer of the reason the account status check is being performed.

[0043] A “token domain” may indicate the factors that can be established at the time of token issuance to enable appropriate usage of the token for payment transactions. Examples of the token domain may include, but are not limited to, a POS entry mode, and merchant identifiers to uniquely identify where the token can be used. A set of parameters (i.e. token domain restriction controls) may be established as part of token issuance by the token service provider that may allow for enforcing appropriate usage of the token in payment transactions. For example, the token domain restriction controls may restrict the use of the token with particular presentment modes, such as contactless or e-commerce presentment modes. In some embodiments, the token domain restriction controls may restrict the use of the token at a particular merchant that can be uniquely identified. Some exemplary token domain restriction controls may require the verification of the presence of a token cryptogram that is unique to a given transaction.

[0044] “Token expiry date” may refer to the expiration date/time of the token. The token expiry date may be passed among the entities of the tokenization ecosystem during transaction processing to ensure interoperability. The token expiration date may be a numeric value (e.g. a 4-digit numeric value).

[0045] A “consumer” may include an individual or a user that may be associated with one or more personal accounts and/or consumer devices. The consumer may also be referred to as a cardholder, account holder, or user.

[0046] An “access device” may be any suitable device for communicating with a merchant computer or payment processing network, and for interacting with a payment device, a user computer apparatus, and/or a user mobile device. An access device may generally be located in any suitable location, such as at the location of a merchant. An access device may be in any suitable form. Some examples of access devices include POS or point of sale devices (e.g., POS terminals), cellular phones, PDAs, personal computers (PCs), tablet PCs, hand-held specialized readers, set-top boxes, electronic cash registers (ECRs), automated teller machines (ATMs), virtual cash registers (VCRs), kiosks, security systems, access systems, Websites on remote server computers, and the like. An access device may use any suitable contact or contactless mode of operation to send or receive data from, or associated with, a payment device and/or a user mobile device.

[0047] In some embodiments, the access device may be a POS terminal. A POS terminal may include a payment device reader, a processor, and a computer-readable medium. The reader may utilize any suitable contact or contactless mode of operation. For example, exemplary card readers can include radio frequency (RF) antennas, optical scanners, bar code readers, or magnetic stripe readers.

[0048] An “authorization request message” may be an electronic message that is sent to a payment processing network and/or an issuer of a payment card to request authorization for a transaction. An authorization request message according to some embodiments may comply with ISO 8583, which is a standard for systems that exchange electronic transaction information associated with a payment made by a consumer using a payment device or payment account. The authorization request message may include an issuer account identifier that may be associated with a payment device or payment account. An authorization request message may also comprise additional data elements corresponding to “identification information” including, by way of example only: a service code, a CVV (card verification value), a dCVV (dynamic card verification value), a PAN (primary account number or “account number”), a user name, an expiration date, etc. An authorization request message may also comprise “transaction information,” such as any information associated with a current transaction, such as the transaction amount, merchant identifier, merchant location, acquirer bank identification number (BIN), card acceptor ID, etc., as well as any other information that may be utilized in determining whether to identify and/or authorize a transaction.

[0049] An “authorization response message” may be an electronic message reply to an authorization request message generated by an issuing financial institution or a payment processing network. The authorization response message may include, by way of example only, one or more of the following status indicators: Approval—transaction was approved; Decline—transaction was not approved; or Call Center—response pending more information, merchant must call the toll-free authorization phone number. The authorization response message may also include an authorization code, which may be a code that a credit card issuing bank returns in response to an authorization request message in an electronic message (either directly or through the payment processing network) to the merchant’s access device (e.g. POS equipment) that indicates approval of the transaction. The code may serve as proof of authorization. As noted above, in some embodiments, a payment processing network may generate or forward the authorization response message to the merchant.

[0050] A “server computer” may include 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 server computer may be coupled to a database and may include any hardware, software, other logic, or combination of the preceding for servicing the requests from one or more client computers. The server computer may comprise one or more computational apparatuses and may use any of a variety of computing structures, arrangements, and compilations for servicing the requests from one or more client computers.

[0051] An “issuer” may typically refer to a business entity (e.g., a bank) that maintains an account for a user that is associated with a portable communication device such as an account enrolled in a mobile application installed on a portable communication device.

[0052] A “merchant” may typically be an entity that engages in transactions and can sell goods or services, or provide access to goods or services.

[0053] An “acquirer” may typically be a business entity (e.g., a commercial bank) that has a business relationship with a particular merchant or other entity. Some entities can perform both issuer and acquirer functions. Some embodiments may encompass such single entity issuer-acquirers.

[0054] FIG. 1 shows a system 100 comprising a number of components. The system 100 comprises a token vault 110, which may be an example of at least part of a token service provider computer. The token vault 110 may be in communication with one or more of a token requestor 115, a merchant 130, an acquirer 135, a payment processing network 140, and an issuer 150. Each of the token requestor 115, the merchant 130, the acquirer 135, the payment processing network 140, and the issuer 150 may be embodied by one or more computers.

[0055] The consumer 120 (i.e., a device operated by the consumer 120) may be in communication with the token requestor 115, the issuer 150, and the merchant 130. Furthermore, the merchant 130, the acquirer 135, the payment processing network 140, the issuer 150, and a token network 145 may all be in operative communication with each other through any suitable communication channel or communications network. A suitable communications network may be any one and/or the combination of the following: a direct interconnection; the Internet; a Local Area Network (LAN); a Metropolitan Area Network (MAN); an Operating Missions as Nodes on the Internet (OMNI); a secured custom connection; a Wide Area Network (WAN); a wireless network (e.g., employing protocols such as, but not limited to a Wireless Application Protocol (WAP), I-mode, and/or the like); and/or the like.

[0056] The token vault 110 may be associated with the payment processing network 140, the issuer 150, the acquirer 135, or the merchant 130. The token vault 110 can receive a token request from the token requestor 115, the request including information (e.g., a PAN) that identifies a payment account. The token vault 110 can issue a token that can be used as surrogate payment account information. A record of the token may be stored at the token vault 110, and the record may include the token, token expiration date, associated payment account information, token assurance information, token requestor information, and/or any other suitable information.

[0057] The token vault 110 may also generate a unique non-transactable payment account identifier that may be a static non-payment identifier. The token vault 110 may associate the non-transactable payment account identifier with a PAN, so that the non-transactable payment account identifier is associated with a payment account.

[0058] In addition to providing the token, the token vault 110 may provide a non-transactable payment account identifier to the token requestor 115 in response to a token request. Thus, the token vault 110 can provide both payment information (via a token) and identification (via a non-transactable payment account identifier) without providing the actual PAN associated with the payment account. In some embodiments, the non-transactable payment account identifier may first be generated and associated with the payment account the first time a token is requested for the payment account. The non-transactable payment account identifier may be identified and provided along with tokens in response to any future token requests.

[0059] The token vault 110 may also be capable of de-tokenizing a token and providing payment account informa-

tion in response to receiving the token. For example, the token vault 110 may receive requests for payment account information from the payment processing network 140, issuer 150, acquirer 135, and/or merchant 130. The token vault 110 may receive a de-tokenization request including a token, identify payment account information that is associated with the token, and provide the payment account information to the de-tokenization requestor.

[0060] The token vault 110 may be an example of a token service computer. The token service computer may comprise a processor and a computer readable medium. The computer readable medium comprising code, executable by the processor, for implementing a method. The method comprises receiving a token request comprising a primary account identifier from a token requestor computer, determining a transactable payment token and a non-transactable payment account identifier associated with the primary account identifier, and transmitting the transactable payment token and the non-transactable payment account identifier to the token requestor computer. If the token requestor computer is not a payment device, the token requestor computer passes the transactable payment token and the non-transactable payment account identifier to the payment device. The transactable payment token and the non-transactable payment account identifier are both passed from the consumer's payment device to an access device to conduct a transaction. The transactable payment token is used by the access device to process a payment for the transaction instead of the primary account identifier. The non-transactable payment account identifier is used as a reference for the primary account identifier to perform an operation that is not a payment transaction.

[0061] In some embodiments, the de-tokenization requestor may be the payment processing network 140, which may request the payment account information for authorization purposes. In some embodiments, the de-tokenization requestor may be the merchant 130 which may wish to have the payment account information for consumer 120 identification purposes.

[0062] The token requestor 115 may request a token on behalf of the consumer 120. The token requestor 115 may be a digital wallet provider, a merchant 130, payment processing network 140, a payment device (e.g., the consumer's mobile phone), or any other suitable entity. The consumer 120 may wish to purchase a good and/or service from the merchant 130 and the token requestor 115 may retrieve a token from the token vault 110 for the consumer 120 to use for the purchase.

[0063] The merchant 130 is capable providing goods and/or services to the consumer 120. In some embodiments, the merchant 130 may receive payment information comprising a token and a non-transactable payment account identifier from the consumer 120 (i.e., a payment device operated by the consumer 120) in a payment transaction. After receiving the token and the non-transactable payment account identifier, the merchant 130 may send the token and the non-transactable payment account identifier to the acquirer 135 for payment authorization.

[0064] In some embodiments, the merchant 130 may use the non-transactable payment account identifier for tracking consumer activity. The non-transactable payment account identifier may be static, so that the same non-transactable payment account identifier is provided each time a consumer 120 uses a certain payment account at a merchant 130, even

if the token is variable. For example, in some embodiments, one payment account may be associated with several digital wallets, and each digital wallet may have a different token associated with the same payment account. The merchant **130** may receive the same non-transactable payment account identifier whenever any of these different tokens are received. Thus, the merchant **130** may be able to recognize a payment account by a received non-transactable payment account identifier. It is also possible for the merchant **130** (or other party) to request that the consumer that is associated with the non-transactable account identifier provide additional information about the consumer (e.g., name, home address, telephone number, zip code, etc.) so that the merchant **130** has additional information to link the consumer to the non-transactable account identifier.

[0065] The merchant **130** may use the non-transactable payment account identifier as a consumer identifier instead of a PAN. The merchant **130** may keep a record of consumer **120** trends by recording transactions that involve the non-transactable payment account identifier. In some embodiments, the non-transactable payment account identifier may comprise 16, 18, or 19 digits and can be formatted as a PAN so that merchants **130** can easily integrate a non-transactable payment account identifier into an existing consumer-tracking system that typically uses a PAN for consumer tracking. The non-transactable payment account identifier may replace a PAN for any suitable identification purpose. A consumer **120** may have more than one payment account, and thus the consumer **120** may be associated with multiple non-transactable payment account identifiers. A non-transactable payment account identifier may also be formatted to indicate an issuer **150** and/or a token vault **110**.

[0066] In some embodiments, the merchant **130** may use the non-transactable payment account identifier and associated consumer purchase record for other applications including value added services such as loyalty programs, backend applications, and reporting. For example, the non-transactable payment account identifier may function as a consumer **120** loyalty identifier for tracking loyalty points and providing rewards or special offers.

[0067] The merchant **130** (or other entity) may also use the non-transactable payment account identifier for fraud/risk checks during authorization. For example, the merchant **130** may be able to detect high-velocity transactions. If too many transactions (associated with the same payment token or multiple payment tokens corresponding to an underlying real account identifier) associated with the non-transactable payment account identifier occur within a certain amount of time, the merchant **130** may suspect fraudulent activity. The merchant may then reject further transactions involving the non-transactable payment account identifier. Alternatively, the merchant **130** may mark the non-transactable payment account identifier as high-risk or put the non-transactable payment account identifier on a “blacklist.” The merchant **130** may also use the non-transactable payment account identifier to review fraud/risk levels after a transaction is authorized.

[0068] The merchant **130** may use the non-transactable payment account identifier to access past transactions. For example, the merchant **130** may use the non-transactable payment account identifier to identify a past transaction for a refund or an inquiry.

[0069] The non-transactable payment account identifier may also be used for providing a transaction feed to third

party value added applications. For example, the merchant **130** may inform third party applications about consumer **120** purchases and trends that are tracked via the non-transactable payment account identifier. A third-party may use a transaction feed for providing rewards or offers to the consumer in real time or offline (e.g. in a statement of credit).

[0070] The acquirer **135** may be associated with the merchant **130**, and may manage authorization requests on behalf of the merchant **130**. The acquirer **135** may receive an authorization request message including the token and non-transactable payment account identifier from the merchant **130** and send the authorization request message to a payment processing network **140**. The payment processing network **140** may be associated with the token and may be identified by one or more fields within the token.

[0071] The acquirer **135** may use the non-transactable payment account identifier for online fraud analysis, offline fraud analysis, loyalty services, third party loyalty programs, reporting to merchants, or any other suitable purpose. For example, in some embodiments, the acquirer **135** may flag a payment account (identified by a non-transactable payment account identifier) and an associated merchant **130** for fraud/risk level scoring. In another example, a non-transactable payment account identifier may be used for providing card-linked offers. In another example, the acquirer **135** may provide a consumer transaction report to merchants, the report including transactions that involved a certain non-transactable payment account identifier.

[0072] In some embodiments, the merchant **130** and/or the acquirer **135** may be able to provide a non-transactable payment account identifier to the token vault **110** and then receive associated payment account information. Additionally, in some embodiments, the merchant **130** and/or the acquirer **135** may provide payment account information to the token vault **110**, and then receive an associated non-transactable payment account identifier. For example, a merchant **130** may send a “Get PAN” request that includes the non-transactable payment account identifier to the token vault **110**, and the token vault **110** may respond with the PAN information. Alternatively, the merchant **130** may send a “Get non-transactable payment account identifier” request including the PAN and/or the transactable payment token to the token vault **110**, and receive a non-transactable payment account identifier associated with the PAN.

[0073] The acquirer **135**, the payment processing network **140**, and the issuer **150**, may operate suitable routing tables to route authorization request messages using real account identifiers such as PANs or tokens. Token routing data may be provided or maintained by the token vault **110**, and may be communicated to any of the entities in FIG. 1.

[0074] The payment processing network **140** may be disposed between the acquirer **135** and the issuer **150**. The payment processing network **140** may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. For example, the payment processing network **140** may comprise a server computer, coupled to a network interface (e.g. by an external communication interface), and a database(s) of information. 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. The payment processing network 140 may use any suitable wired or wireless network, including the Internet.

[0075] The payment processing network 140 may be able to de-tokenize any tokens in any authorization request message that is received. For example, the payment processing network 140 may receive an authorization request message including a token and non-transactable payment account identifier, send the token and non-transactable payment account identifier to the token vault 110, receive associated payment account information from the token vault 110, and forward the authorization request message to the issuer 150 with the payment account information. The payment processing network 140 may also receive an authorization response message with the payment account information, and replace some or all of the payment account information with the token and/or non-transactable payment account identifier before forwarding the message to the acquirer 135.

[0076] In some embodiments, the token vault 110 and the payment processing network 140 may form a token service system. The token service system comprises a token service computer comprising a first processor and a first computer readable medium, the first computer readable medium comprising code, executable by the first processor to implement a method. The method includes receiving a token request associated with account information, determining a non-transactable payment account identifier and a transactable payment token associated with the account information, and providing the non-transactable payment account identifier and the transactable payment token associated with the account information. The method also includes a payment processing network computer in communication with the token service computer. The payment processing network computer comprises a second processor and a second computer readable medium, the second computer readable medium comprising code, executable by the second processor for implementing a method. The method comprises receiving an authorization request message including the transactable payment token and the non-transactable payment account identifier from a merchant, adding the account information to the authorization request message, sending the authorization request message to an issuer, receiving an authorization response message including the account information from the issuer, replacing the account information with the transactable payment token and the non-transactable payment account identifier in the authorization response message, and sending the authorization response message to the merchant.

[0077] The token network 145 may also be able to provide de-tokenization services. The token network 145 may include another payment processing network, another token vault, and/or another token requestor. For example, in some embodiments, the consumer 120 may receive a token that is associated with a payment processing network of the token network 145. In order to de-tokenize the token for authorization, the payment processing network 140 may send the token and non-transactable payment account identifier to the token network 145, which may then return the payment account information. In some embodiments, the token network 145 may wish to de-tokenize a token that is associated

with the payment processing network 140, and may obtain associated payment account information by similarly communicating with the payment processing network 140 and token vault 110.

[0078] A method 200 according to embodiments of the invention can be described with respect to FIG. 2. The steps shown in the method 200 may be performed sequentially or in any suitable order in embodiments of the invention.

[0079] In a purchase transaction, the consumer 120 may purchase a good or service at a merchant 130. The merchant 130 may then request that the consumer 120 provide payment information to conduct the purchase. Instead of providing a credit card number to the merchant 130, the consumer 120 can use a token to conduct the payment transaction. The consumer 120 may cause the token requestor 115 to request a token to conduct the transaction. In this example, the token requestor 115 may be the consumer's mobile phone or may be a digital wallet that is associated with the consumer's mobile phone. The token requestor 115 may then send a token request to the token vault 110 on behalf of the consumer 120.

[0080] The token may be requested or provided using any suitable form of communication. In some embodiments, a token request may be in an electronic message format, such as an e-mail, a short messaging service (SMS) message, a multimedia messaging service (MMS) message, a hypertext transfer protocol (HTTP) request message, a transmission control protocol (TCP) packet, a web form submission. The token request may be directed to any suitable location, such as an e-mail address, a telephone number, an internet protocol (IP) address, or a uniform resource locator (URL). In some embodiments, a token request may comprise a mix of different message types, such as both email and SMS messages.

[0081] Further, the token request may include any suitable type of information. For example, the token request may include an account identifier (e.g., a PAN) associated with an account that is to be used to pay for the good or service, a token requestor ID, or any other suitable information.

[0082] In step S210, the token vault 110 may receive the token request from the token requestor 115. As noted above, the token request may include information about the payment account for which a token is desired.

[0083] In step S220, in response to the token request, the token vault 110 may determine (e.g., generate or identify) a non-transactable payment account identifier and associate the non-transactable payment account identifier with the payment account information of the consumer 120. The token vault 110 may store a record of the non-transactable payment account identifier and associated payment account information in a database if desired.

[0084] The non-transactable payment account identifier may be determined in any suitable manner. For example, the non-transactable payment account identifier may be generated using an algorithm that converts a real PAN into the non-transactable payment account identifier. In some embodiments, the algorithm may be an encryption algorithm such as DES, triple DES, etc. In another example, a listing of non-transactable payment account identifiers may be generated in advance and a non-transactable payment account identifier could be assigned to each received token request.

[0085] In step S230, the token vault 110 may then determine (e.g., identify or generate) a token that represents or is

associated with the indicated payment account information. The token vault **110** may maintain a record including the account information, the token associated with the account information, the non-transactable payment account identifier associated with the account information, a token expiration date, a token assurance level, and/or any other suitable information in a database.

[0086] The token may be determined in any suitable manner. For example, the non-transactable payment account identifier may be generated using an algorithm that converts a real PAN into the token. In another example, a listing of tokens may be generated in advance and a token could be assigned to each received token request.

[0087] In step **S240**, the token vault **110** may then transmit the token and the non-transactable payment account identifier to the token requestor **115** in a token response message. In other embodiments, the token and the non-transactable token may be transmitted to the token requestor **115** in multiple messages. The token response message may have the same or different form or format as the previously described token request message. It may also have additional information that was not present in the token request message. For example, the token response message may include other information such as the time period in which the token would be valid.

[0088] The token requestor **115** may provide the information to the consumer **120** (i.e., a payment device operated by the consumer **120**), which may then provide the token and non-transactable payment account identifier to the merchant **130**. Or, the token requestor **115** may provide the information to the merchant **130**. Any suitable mode of communication may be used to provide the information to the merchant **130**.

[0089] As will be described in further detail below, in some embodiments, the token is provided as payment information and the non-transactable payment account identifier is provided as extended token data or additional VAS data. In some embodiments, the token requestor **115** or consumer **120** may generate a QR code that may include the token and the non-transactable payment account identifier in a transaction payload. The consumer **120** may provide the QR code to the merchant **130** via an access device. Any other suitable communication mechanism (e.g., a contactless mechanism) may be used to pass the token and the non-transactable payment account identifier (as well as any other transaction information) to the merchant.

[0090] In some embodiments, the merchant **130** may then use the non-transactable payment account identifier to identify a purchase record of the consumer **120** and may update the record with the current transaction. The merchant **130** may use the non-transactable payment account identifier-identified consumer **120** record for various applications including online fraud analysis, offline fraud analysis, value added services (e.g. loyalty, backend applications, reporting), third-party transaction feeds, or any other suitable purposes.

[0091] The merchant **130** may forward the token, the non-transactable payment account identifier, and other information to the acquirer **135** in an authorization request message. The token may be in the data field in the authorization request message normally reserved for the PAN, while the non-transactable payment account identifier may be placed in a supplemental or discretionary data field such

as Field **55**. If desired, the data in the supplemental discretionary data field may follow a tag-length-value data format.

[0092] The acquirer **135**, in turn, may send the authorization request message to the payment processing network **140**. The acquirer **135** may also use the non-transactable payment account identifier for identifying the consumer **120**, online fraud analysis, offline fraud analysis, loyalty services, third party loyalty programs, value added services (e.g. loyalty, backend applications), third-party transaction feeds, reporting to merchants, or any other suitable purposes.

[0093] In step **S250**, the payment processing network **140** may receive the authorization request message. After the payment processing network **140** receives the authorization request message, it extracts the token from the authorization request message and then de-tokenizes it. In some embodiments, it can do this by requesting the payment account information from the token vault **110**. In some embodiments, if the token is associated with another payment processing network that is a part of a different token network **145**, the payment processing network **140** may request the payment account information from the token network **145**.

[0094] The token vault **110** may receive the token and/or non-transactable payment account identifier from the payment processing network **140**. In step **S260**, the token vault **110** may identify the associated payment account information in the token record, and send the payment account information to the payment processing network **140**.

[0095] In step **S270**, the payment processing network **140** may replace the token in the authorization request message with the payment account information. For example, if the account information includes a PAN, then the token is removed from the PAN data field in the authorization request message. The PAN is then added back into the authorization request message. The non-transactable payment account identifier may remain in a supplemental data field. Once this is done, the payment processing network **140** may forward the authorization request message to the issuer **150**.

[0096] After the issuer **150** receives the authorization request message, the issuer **150** may analyze it and may determine whether or not to authorize the transaction. The issuer **150** may determine if the account associated with the authorization request message has sufficient funds or credit. It may also determine that the transaction is not inherently risky. If the transaction is authorized by the issuer **150**, the issuer **150** may send an authorization response including the payment account information and an approval code to the payment processing network **140**.

[0097] In step **S280**, the payment processing network **140** receives the authorization response message including the payment account information from the issuer **150**. The payment processing network **140** may then query the token vault **110** for information associated with the payment account information, such as the token and non-transactable payment account identifier. The token vault **110** may identify the requested information in the token record and provide it to the payment processing network **140**.

[0098] In step **S290**, the payment processing network **140** may add the token, non-transactable payment account identifier, or any other suitable transaction information into the authorization response message, and may remove some or all of the payment account information from the message. For example, in some embodiments, the last four digits of a PAN may remain in the message, even though the real PAN

is removed and is replaced with the token. The non-transactable payment account identifier may remain in a supplemental data field.

[0099] In step S295, the payment processing network 140 may then forward the message to the acquirer 135. The acquirer 135 may forward the message to the merchant 130, which may inform the consumer 120 of the authorization results. The merchant 130 may update the non-transactable payment account identifier-identified consumer 120 transaction record with the authorization results.

[0100] At the end of the day or at some other predetermined interval of time, a clearing and settlement process between the issuer 150, the payment processing network 140, and the acquirer 135 may occur. In the clearing and settlement process, account information and token exchanges that are similar to those in the above-described authorization processing steps can occur.

[0101] Subsequent transactions using different transactable payment tokens using the same payment device may use the same non-transactable payment account identifier.

[0102] As shown above, because the non-transactable payment account identifier passes through a number of entities in the payments system, each of those entities may retrieve, store, analyze, and process the transaction data associated with the non-transactable payment account identifier. This is the case, even though different payment tokens are used for different transactions conducted with the same underlying account or payment device.

[0103] FIG. 3 shows a block diagram of another embodiment of the invention. FIG. 3 shows a diagram of a more detailed system that can incorporate a non-transactable payment account identifier.

[0104] FIG. 3 shows a payment device 302 and a POS terminal 306 (which is an example of an access device) which may be located at a merchant. The POS terminal 306 may communicate with an acquirer computer 310, a payment processing network 312, and an issuer computer 314.

[0105] The payment device 302 may be in communication with a wallet server computer 316, which may comprise a value added services module (which may include VAS data) 316A and a payment module 316B. The wallet server computer 316 may communicate with an external value added services computer 318 as well as a cloud based payments platform 320 and a tokenization service computer 322. The tokenization service computer 322 may communicate with the payment processing network 312.

[0106] The payment device 302 may comprise a data transmit application 302A and a mobile wallet application 302B. For clarity of illustration, some of the hardware and software elements in the payment device 302 are not shown in FIG. 3. The payment device 302 may additionally include a data processor, and a communication interface (e.g., a contactless interface), a memory, a computer readable medium, input devices (e.g., input keys, a microphone, etc.), output devices (e.g., a touchscreen, speaker, etc.), and an antenna (e.g., for long range communication). The payment device 302 may be in the form of a payment card, a key fob, a mobile phone, a tablet computer, a wearable device, etc.

[0107] The POS terminal 306 may comprise a data receive application 306A, a payment API (application program interface) 306B, a POS shopping application 306C, and a local value added services (VAS) application 306D. For clarity of illustration, some of the hardware and software elements in the POS terminal 306 are not shown in FIG. 3.

The POS terminal 306 may additionally include a data processor, and a communication interface (e.g., a contactless interface, a data reader such as a card reader), a memory, a computer readable medium, input devices (e.g., input keys, a microphone, etc.), output devices (e.g., a touchscreen, speaker, etc.), and an antenna (e.g., for long range communication).

[0108] The wallet server 316 may comprise a data processor, a memory and a computer readable medium. The VAS module 316A and the payment module 316B may reside in the memory and/or the computer readable medium. The wallet server 316 may store payment account data (e.g., transactable payment tokens) that may be used by the payment device 302 to conduct purchase transactions.

[0109] The external value added services computer 318 may be operated by an entity that is different than the other entities shown in FIG. 3. It may provide value added data (described above and below) to the wallet server 316 and the payment device 302.

[0110] The cloud based payments platform 320 may include a gateway that supplies transactable payment tokens, non-transactable payment account identifiers and other information directly or indirectly to the payment device 302.

[0111] The tokenization service computer 322 can perform tokenization services and can include the above described token vault.

[0112] FIG. 4 shows a flow diagram illustrating methods that can be used with the system illustrated in FIG. 3. In particular, methods illustrating the use of the non-transactable account identifier with value added services data can be described with reference to FIGS. 3 and 4.

[0113] In embodiments of the invention, non-payment data can be provided by merchant or third party applications, which may be used primarily by a merchant POS terminal (and optionally by an acquirer) to provide value added services to consumers. Merchants prefer to have non-payment information (e.g., loyalty IDs, coupon IDs, order numbers, etc.) with payment credentials to provide value added services. Merchants currently get this information in different forms (e.g., manually, cards, multiple apps, etc.) through multiple consumer interactions. This mode of providing such non-payment information is inconvenient for consumers. As illustrated below, embodiments of the invention can combine non-payment data from one or more data sources with payment data in a single data element, which may be transmitted from a payment device to a POS terminal.

[0114] Referring to FIG. 4, in step S400, a wallet application 302B in a payment device 302 (e.g., a mobile phone) may send a token request to a tokenization service computer 322. The token request may include an account identifier such as a PAN or some other identifier related to the account. Further details on token requests are provided above.

[0115] In step S402, after the token request is received by the tokenization service computer 322, the tokenization service computer 322 performs any desired fraud or status checks on the token request. If the checks indicate that a token can be issued, the tokenization service computer 322 can transmit a token to the wallet application 302B in the payment device 302. In addition to the token, the tokenization service computer 322 may transmit other information including one or more of a token expiration date, a token requestor ID, a digital wallet ID, and a non-transactable payment account identifier to the wallet application 302B on

the payment device **302**. The token and the other information may be transmitted to the wallet application **302B** in the payment device **302** in a single communication or in multiple communications.

[0116] In step **S404**, before or after step **S402**, one or more value added service data sources **316A**, **318** may directly or indirectly transmit value added service data to the wallet application **302B** on the payment device **302**. The data sources may include value added services data **316A** from the wallet server **316** or value added data from the external value added services computer **318**. Examples of value added services data may include one or more of a loyalty identifier (e.g., a frequent flier account number) held by the consumer, a coupon identifier, and an order number for a past or current purchase.

[0117] The wallet application **302B** passes the data from the token service computer **322** and the value added service data source(s) **316**, **318** to the data transmit application **302A** in the payment device **302A**. The data transmit application **302A** operating in conjunction with a data processor on the payment device **302A** generates a transaction payload and it may be in the form of a data element such as a QR code. Other data elements such as a cryptogram may be generated by the payment device **302A** and may be included in the transaction payload. By incorporating value added services data from the wallet application **302B** in the payment device **302** with the token, value added services that can benefit the consumer or others can be easily provided at the point of transaction.

[0118] The value added services data may be in any suitable form, and may include any suitable type of data. It may include strings of characters, image files, videos, etc. Each piece of value added data may have a tag value associated with it. The tag may be defined by the entity (e.g., a payment processing network) that originates or processes the value added services data. Table 1 below provides examples of value added services data.

TABLE 1

Exemplary value added services data list		
Value added services data	Description	Data Type
Merchant loyalty ID	Loyalty ID issued by a merchant and processed at a POS terminal	Alphanumeric
Alternate loyalty credential - e-mail	Loyalty ID in the form of a consumer e-mail address	E-mail address
Alternate loyalty credential - phone	Loyalty ID in the form of a phone number	Numeric
Order confirmation	Order number placed by consumer at merchant - for remote order and pickup	Alphanumeric
Offer code	Coupon/Offer code locally redeemable by the merchant POS terminal	Numeric
Employee ID	Employee ID at retailer which makes them eligible for special discounts	Alphanumeric
Zip code	Zip code which may be used for data analysis	Numeric
Ticket number	Ticket number which may be processed by a POS terminal	Alpha Numeric

TABLE 1-continued

Exemplary value added services data list		
Value added services data	Description	Data Type
Token Requestor (Wallet) URL	URL of Token Requestor (Wallet) Service for merchant POS to close the loop	URL

[0119] After the wallet application **302B** receives the value added services data, the token, the non-transactable account identifier, and any other suitable information in the token response from the tokenization service computer **322**, the data transmit application **302A** may obtain and consolidate this information into a single data element. The single data element can be transmitted to the POS terminal **306** at the merchant. For instance, the data transmit application **302A** may be a QR code generation module, which may generate a single QR code which encodes the token, the non-transactable account identifier, and any value added services data. Other information that may be included in the single data element may include cryptograms or other information that may be generated by the payment device **302**. In other embodiments, multiple data elements can be generated to encode the token and its associated data, as well as the value added services data.

[0120] After the single data element is generated by the payment device **302**, in step **S406**, it is then passed to data receive application **306A** in the POS terminal **306**. The data receive application **306A**, working in conjunction with a data processor in the POS terminal **306**, may then convert the single data element into the original data that was used to form the single data element. The POS shopping application **306C** in the POS terminal **306** can then optionally retrieve any additional value added service data (e.g., coupons) from a local value added service data store **306D** or from the external value added services computer **318**, and can perform any desired processing. For example, in some embodiments, the value added services data could be a coupon that is redeemable at the merchant that operates the POS terminal **306**. The POS shopping application **306C** may reduce the amount of the transaction by the value of the coupon when generating an authorization request message for the amount that will be owed by the consumer when conducting the transaction.

[0121] After the POS shopping application determines the amount of the payment transaction, the POS terminal **306** then generates an authorization request message comprising at least some of the elements in the transaction payload received from the payment device **302**. The token may be in the data field in the authorization request message normally reserved for the PAN, while the non-transactable payment account identifier may be placed in a supplemental or discretionary data field such as Field **55**. If desired, the data in the supplemental discretionary data field may follow a tag-length-value data format.

[0122] In step **S408**, the authorization request message is transmitted by the POS terminal **306** via the payment API **306B** to the acquirer computer **310**. The authorization request message may comprise any suitable data including the token and the non-transactable payment account identifier. It may also include the token expiration date, the cryptogram from the payment device **302**, the token requestor identifier, the digital wallet identifier, and a POS terminal entry mode.

[0123] The POS terminal entry mode may identify the mode in which the POS terminal 306 received the transaction payload from the payment device 302. For example, the POS terminal entry mode may indicate that a QR code was the mechanism that was used to transmit the transaction payload from the payment device 302 to the POS terminal 306. This information can be useful to a downstream payment processor. For example, some modes of data transmission are inherently more secure or reliable than other modes of data transmission. This information can be used, for example, to improve transaction fraud scoring.

[0124] In step S410, after receiving the authorization request message from the POS terminal 306, the authorization request message is then transmitted from the acquirer computer 310 to the payment processing network 312.

[0125] After the payment processing network 312 receives the authorization request message, it may then alter the authorization request message. For example, a computer in the payment processing network 312 may provide the token, the token expiration date, and any other appropriate information to the tokenization service computer 322. If the token is valid, the tokenization service computer 322 may then provide the real account identifier to the payment processing network 312. The payment processing network can then replace the token and the token expiration date in the authorization request message with the real account identifier (e.g., a PAN) and the expiration date for the real account identifier.

[0126] In step S412, the modified authorization request message is then transmitted by the payment processing network 312 to the issuer computer 314.

[0127] The issuer computer 314 then determines whether or not the transaction should be authorized. It may conduct any appropriate fraud or credit checks to determine whether or not to approve of the transaction. After this analysis occurs, in step S414, the issuer computer 314 then generates and sends an authorization response message comprising the real account identifier back to the payment processing network computer 312.

[0128] The payment processing network 312 may then substitute the token for the real account identifier in the authorization response message. The payment processing network 312 may also provide other information in the authorization response message including, but not limited to a PAN product ID (e.g., an ID that indicates that the PAN is associated with a credit card with a higher customer status), the last four digits of the real account identifier, the token assurance level, the non-transactable payment account identifier, and the token requestor identifier.

[0129] In step S416, after the payment processing network 312 modifies the authorization response message, the payment processing network 312 may transmit the modified authorization response message to the acquirer computer 310.

[0130] In step S418, after the acquirer computer 310 receives the authorization response message, the acquirer computer 310 may transmit the authorization response message to the POS terminal 306.

[0131] At the end of the day or at some other predetermined interval of time, a clearing and settlement process between the issuer computer 314, the payment processing network 312, and the acquirer computer 310 may occur. In the clearing and settlement process, account information and

token exchanges that are similar to those in the above-described authorization processing steps can occur.

[0132] Subsequent transactions using different transactable payment tokens using the same payment device may use the same non-transactable payment account identifier.

[0133] As shown above, because the non-transactable payment account identifier passes through a number of entities in the payments system, each of those entities may retrieve, store, analyze, and process the transaction data associated with the non-transactable payment account identifier. This is the case, even though different payment tokens are used for different transactions conducted with the same underlying account or payment device.

[0134] Embodiments of the invention have a number of advantages. For example, the non-transactable payment account identifier allows merchants to track consumer spending habits, analyze fraud/risk, provide transaction feeds to third party applications, etc. without requiring sensitive payment account information, such as a PAN. Thus, tokens may be used to make a consumer's payment account information more secure without interfering with a merchant's programs. Instead of tracking a payment account by several digital wallet-specific tokens, potentially leading to multiple detached records for one consumer, the merchant (or other entity) may be able to aggregate all token spending records for one payment account via the non-transactable payment account identifier.

[0135] FIG. 5 is a high level block diagram of a computer system that may be used to implement any of the entities or components described above. The subsystems shown in FIG. 5 are interconnected via a system bus 500. Additional subsystems include a printer 508, keyboard 516, fixed disk 518, and monitor 512, which is coupled to display adapter 510. Peripherals and input/output (I/O) devices, which couple to I/O controller 502, can be connected to the computer system by any number of means known in the art, such as a serial port. For example, serial port 514 or external interface 520 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 300 allows the central processor 506 to communicate with each subsystem and to control the execution of instructions from system memory 504 or the fixed disk 518, as well as the exchange of information between subsystems. The system memory 504 and/or the fixed disk may embody a computer-readable medium.

[0136] 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.

[0137] 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 tech-

niques. 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.

[0138] 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.

[0139] As used herein, the use of “a”, “an” or “the” is intended to mean “at least one”, unless specifically indicated to the contrary.

1.-20. (canceled)

21. A method comprising:

receiving, by a computer, a request comprising a non-transactable payment account identifier from an entity of one or more entities;

determining, by the computer, information associated with the non-transactable payment account identifier; and

transmitting, by the computer, the information associated with the non-transactable payment account identifier to the entity.

22. The method of claim **21**, wherein the non-transactable payment account identifier is formatted as a primary account number.

23. The method of claim **21**, wherein the non-transactable payment account identifier is static over time and over any number of transactions.

24. The method of claim **21**, wherein the one or more entities comprises a payment processing network configured to process credit and debit card transactions.

25. The method of claim **21**, wherein the request comprises a token associated with the non-transactable payment account identifier.

26. The method of claim **21**, wherein the request is an authorization request message, and wherein the entity is an acquirer computer.

27. The method of claim **21**, wherein the information associated with the non-transactable payment account identifier includes a primary account number.

28. A method comprising:

receiving a request comprising a primary account identifier from a token requestor computer;

determining a transactable payment token and a non-transactable payment account identifier associated with the primary account identifier; and

transmitting the transactable payment token and the non-transactable payment account identifier to the token requestor computer.

29. The method of claim **28**, wherein the non-transactable payment account identifier is static over time and over any number of transactions.

30. The method of claim **28**, wherein the non-transactable payment account identifier is formatted as a primary account number.

31. The method of claim **28**, further comprising:

associating and storing the primary account identifier and the non-transactable payment account identifier in a database.

32. The method of claim **28**, wherein the non-transactable payment account identifier is mathematically derived from the primary account identifier.

33. The method of claim **28**, wherein the token requestor computer is a mobile device operated by a user.

34. A computer comprising:

a processor; and

a non-transitory computer readable medium comprising code, executable by the processor for implementing a method comprising:

receiving a request comprising a primary account identifier from a token requestor computer,

determining a transactable payment token and a non-transactable payment account identifier associated with the primary account identifier; and

transmitting the transactable payment token and the non-transactable payment account identifier to the token requestor computer.

35. The computer of claim **34**, wherein the non-transactable payment account identifier is static over time and over any number of transactions.

36. The computer of claim **34**, wherein the non-transactable payment account identifier is formatted as a primary account number.

37. The computer of claim **34**, wherein the method further comprises:

associating and storing the primary account identifier and the non-transactable payment account identifier in a database.

38. The computer of claim **34**, wherein the non-transactable payment account identifier is mathematically derived from the primary account identifier.

39. The method of claim **34**, wherein the token requestor computer is a mobile device operated by a user.

* * * * *