



(86) **Date de dépôt PCT/PCT Filing Date:** 2014/07/24
(87) **Date publication PCT/PCT Publication Date:** 2015/01/29
(85) **Entrée phase nationale/National Entry:** 2016/01/22
(86) **N° demande PCT/PCT Application No.:** US 2014/048038
(87) **N° publication PCT/PCT Publication No.:** 2015/013522
(30) **Priorités/Priorities:** 2013/07/24 (US61/858,087);
2013/08/08 (US61/863,863); 2014/02/03 (US61/935,036)

(51) **Cl.Int./Int.Cl.** **G06Q 20/40** (2012.01),
H04L 9/32 (2006.01), **H04W 12/06** (2009.01)
(71) **Demandeur/Applicant:**
VISA INTERNATIONAL SERVICE ASSOCIATION, US
(72) **Inventeurs/Inventors:**
DILL, MATTHEW, US;
LAXMINARAYANAN, PRASANNA, US;
POWELL, GLENN, US;
SHEETS, JOHN F., US;
CARPENTER, ANDREW, US
(74) **Agent:** BERESKIN & PARR LLP/S.E.N.C.R.L., S.R.L.

(54) **Titre : SYSTEMES ET PROCEDES DE COMMUNICATION D'UN RISQUE AU MOYEN DE DONNEES D'ASSURANCE DE JETON**
(54) **Title: SYSTEMS AND METHODS FOR COMMUNICATING RISK USING TOKEN ASSURANCE DATA**

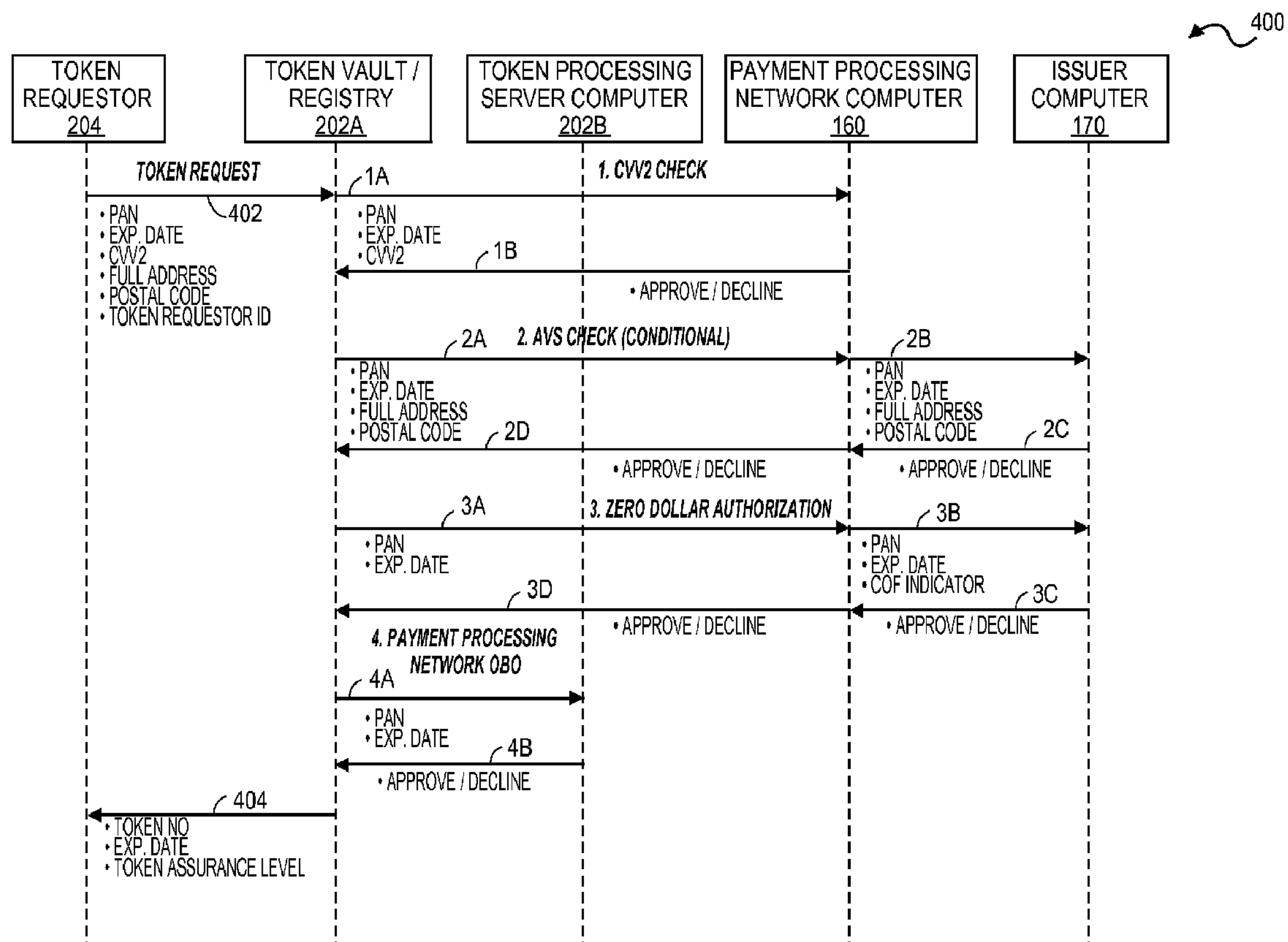


FIG. 4A

(57) **Abrégé/Abstract:**

Systems and methods for communicating risk using token assurance data are provided. A network token system provides a platform that can be leveraged by external entities (e.g., third party wallets, e-commerce merchants, payment enablers / payment



(57) Abrégé(suite)/Abstract(continued):

service providers, etc.) or internal payment processing network systems that have the need to use the tokens to facilitate payment transactions. An authorization request message can include a token assurance level code that is indicative of a token assurance level associated with a generated token. External or internal entities may use the token assurance level to evaluate risk associated with a payment transaction that uses the token.

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

(19) World Intellectual Property
Organization
International Bureau

WIPO | PCT

(10) International Publication Number
WO 2015/013522 A1(43) International Publication Date
29 January 2015 (29.01.2015)

(51) International Patent Classification:

G06Q 20/40 (2012.01) *H04L 9/32* (2006.01)
H04W 12/06 (2009.01)

(21) International Application Number:

PCT/US2014/048038

(22) International Filing Date:

24 July 2014 (24.07.2014)

(25) Filing Language:

English

(26) Publication Language:

English

(30) Priority Data:

61/858,087	24 July 2013 (24.07.2013)	US
61/863,863	8 August 2013 (08.08.2013)	US
61/935,036	3 February 2014 (03.02.2014)	US

(71) Applicant: **VISA INTERNATIONAL SERVICE ASSOCIATION** [US/US]; P.O. Box 8999, San Francisco, California 94128 (US).(72) Inventors: **DILL, Matthew**; 1860 Quail Court, St. Helena, California 94571 (US). **LAXMINARAYANAN, Prasanna**; 3059 Enfield Street, San Ramon, California 94582 (US). **POWELL, Glenn**; 47830 Maya Street, Fremont, California 94539 (US). **SHEETS, John, F.**; 915 Elizabeth Street, San Francisco, California 94114 (US).(74) Agents: **DAVE, Urmil V.** et al.; Kilpatrick Townsend & Stockton LLP, Two Embarcadero Center, 8th Floor, San Francisco, California 94111 (US).(81) Designated States (*unless otherwise indicated, for every kind of national protection available*): AE, AG, AL, AM, AO, AT, AU, AZ, BA, BB, BG, BH, BN, BR, BW, BY, BZ, CA, CH, CL, 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, IR, IS, JP, KE, KG, 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, PA, PE, PG, PH, PL, PT, QA, RO, RS, RU, RW, SA, SC, SD, SE, SG, SK, SL, SM, ST, SV, SY, TH, 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, LR, LS, MW, MZ, NA, RW, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, RU, TJ, TM), European (AL, AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, RS, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, KM, ML, MR, NE, SN, TD, TG).

Published:

— with international search report (Art. 21(3))

(54) Title: SYSTEMS AND METHODS FOR COMMUNICATING RISK USING TOKEN ASSURANCE DATA

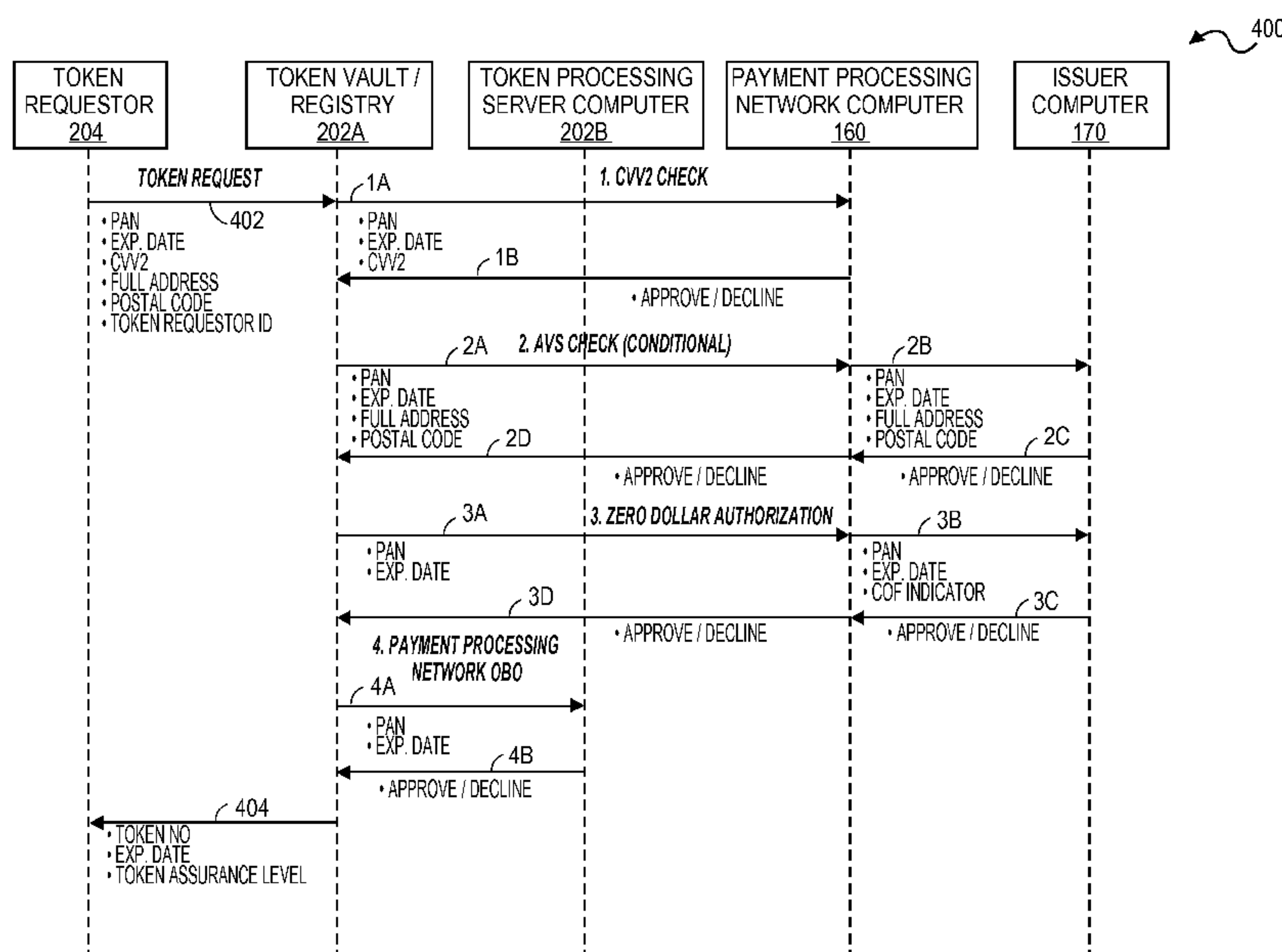


FIG. 4A

(57) Abstract: Systems and methods for communicating risk using token assurance data are provided. A network token system provides a platform that can be leveraged by external entities (e.g., third party wallets, e-commerce merchants, payment enablers / payment service providers, etc.) or internal payment processing network systems that have the need to use the tokens to facilitate payment transactions. An authorization request message can include a token assurance level code that is indicative of a token assurance level associated with a generated token. External or internal entities may use the token assurance level to evaluate risk associated with a payment transaction that uses the token.

SYSTEMS AND METHODS FOR COMMUNICATING RISK USING TOKEN ASSURANCE DATA

CROSS-REFERENCES TO RELATED APPLICATIONS

[0001] This application claims the benefit of priority to U.S. Provisional Application No. 61/858,087, filed on July 24, 2013, U.S. Provisional Application No. 61/863,863, filed on August 8, 2013, and U.S. Provisional Application No. 61/935,036, filed on February 3, 2014, which are herein incorporated by reference in their entirety for all purposes.

[0002] This application is related to U.S. non-provisional patent application no. _____, entitled "SYSTEMS AND METHODS FOR INTEROPERABLE NETWORK TOKEN PROCESSING" (Attorney Docket No. 671US03 (79900-910620)) and U.S. non-provisional patent application no. _____, entitled "SYSTEMS AND METHODS FOR COMMUNICATING TOKEN ATTRIBUTES ASSOCIATED WITH A TOKEN VAULT" (Attorney Docket No. 671US04 (79900-910621)), all of which are filed on the same day as the present application.

BACKGROUND

[0003] In a traditional electronic payment transaction, a consumer's PAN (primary account number) information is exposed to various entities involved during the transaction lifecycle. The PAN is passed from a merchant terminal, to an acquirer system, a payment processing network, payment gateways, etc.

[0004] Because the PAN can be exposed at various points in the transaction lifecycle, some have suggested that payment "tokens" be used to conduct payment transactions. A token serves as an additional security layer to the PAN and in effect becomes a proxy/surrogate to the PAN and may be used in place of PAN while

submitting transactions. The use of payment tokens instead of PANs can reduce the risk of fraudulent activity since the real PAN is never exposed.

[0004] While conventional efforts to use payment tokens have been useful, a number of problems need to be solved. For example, it is relatively straightforward to run traditional authentication processes during a normal transaction with a real PAN, since the consumer data and prior history data for the real PAN can be easily obtained. Consequently, fraud engines in the payment system can determine, during the transaction, if the transaction is fraudulent and/or otherwise risky so that appropriate determinations can be made by the entities involved with the transaction as to whether or not to proceed with the transaction.

[0005] However, because a token is an obfuscated PAN, it is not possible to run the same authentication processes that could otherwise be run with a normal PAN. That is, a merchant, payment processor, or issuer, would receive a token, but could not readily link this token to a specific consumer or payment account. Consequently, the normal authentication and verification processes that would normally occur in a normal payment transaction cannot be easily performed. While it might be possible for some of the entities in the payment system to perform any fraud checking or authentication after the real PAN is obtained from the token (e.g., from a token vault), this process may be too slow or it may defeat the purpose of using a token in the first place, since entities such as the merchant may be receiving and may be in possession of the real PAN.

[0006] Embodiments of the invention address these and other problems, individually and collectively.

BRIEF SUMMARY

[0007] In some embodiments of the invention, a network token system is provided. The network token system provides a platform that can be leveraged by various entities such as third party wallet providers, merchants, acquirers, payment processors, etc. that use tokens to facilitate payment transactions. In the network token system, a token registry vault can provide interfaces for various entities (e.g., mobile

devices, issuers, merchants, mobile wallet providers, acquirers, etc.) to request payment tokens, request information about payment tokens or otherwise process payment tokens. The network token system further provides for services such as a providing a token assurance level. The token assurance level may be represented in the form of a token assurance level code that may be understood by the various entities in the network token system.

[0008] One embodiment of the invention is directed to a method comprising receiving, by a server computer, a token request from a token requester. After the token request is received, the method comprises performing, by the server computer, at least one authentication process associated with the token request. In response to the performance of the at least one authentication process, the method comprises generating, by the server computer, a token assurance code and transmitting, by the server computer, the token to the token requester

[0009] Another embodiment of the invention is directed to a method comprising receiving, by a server computer, an authorization request message comprising a payment token, wherein the payment token is associated with a real account identifier. The method further comprises determining, by the server computer, the real account identifier associated with the payment token. The method also comprises generating, by the server computer, a modified authorization request message comprising the real account identifier, wherein the modified authorization request message comprises a token assurance level code indicative of a level of confidence associated with the payment token. Further, the method comprises transmitting, by the server computer, the modified authorization request message to an issuer for approval.

[0010] Other embodiments of the invention are directed to server computers and systems that are configured to perform the above-described methods.

[0011] In some embodiments, the issuer approval is based at least in part on the token assurance level code.

[0012] In some embodiments, the level of confidence associated with the payment token comprises a level of confidence that the payment token was requested

by an account holder of an underlying payment account associated with the real account identifier.

[0013] In some embodiments, the token assurance level code indicates an authentication method associated with the payment token.

[0014] In some embodiments, the authentication method comprises at least one of: no authentication, network authentication, or issuer authentication.

[0015] In some embodiments, the token assurance level code is based at least in part on a transaction history associated with the real account identifier.

[0016] In some embodiments, the authorization request message is received by the server computer from a merchant computer.

[0017] In some embodiments, the method additionally includes receiving an authorization response message from the issuer, generating a modified authorization response message comprising the payment token and the token assurance level code, and transmitting the modified authorization response message to a merchant computer.

[0018] In some embodiments, before receiving the authorization request message, the payment token is generated and provided to the server computer by an account issuer.

[0019] In some embodiments, the token assurance level code is generated at the time the payment token is generated, before it is generated, or after it is generated.

[0020] These and other embodiments of the invention are described in further detail below.

BRIEF DESCRIPTION OF THE DRAWINGS

[0021] FIG. 1 shows a block diagram of a typical transaction processing system for electronic payment transactions using issuer accounts, in accordance with some embodiments of the invention.

[0022] FIG. 2 shows a block diagram of a transaction processing system utilizing a network token system, in accordance with some embodiments of the invention.

[0023] FIG. 3 shows a block diagram of a token processing server computer, in accordance with some embodiments of the invention.

[0024] FIGs. 4A-4B show exemplary authentication methods that can be used to determine token assurance levels, in accordance with some embodiments of the invention.

[0025] FIG. 5 shows a flow diagram for an exemplary transaction flow for NFC at the point-of-sale, in accordance with some embodiments of the invention.

[0026] FIG. 6 shows a flow diagram for an exemplary flow for a card-on-file/e-commerce transaction, in accordance with some embodiments of the invention.

[0027] FIG. 7 is a flowchart of an exemplary method for transmitting a token assurance level code to an issuer or other entity, in accordance with some embodiments of the invention.

[0028] FIG. 8 shows a block diagram of a computer apparatus.

DETAILED DESCRIPTION

[0029] Embodiments are directed at systems, methods, and devices for communicating risk using a token assurance level. As explained above, tokenization can involve the replacement or exchange of original payment credentials (e.g., a primary account number (PAN)) for substitute data (e.g., a non-financial identifier or a substitute PAN). A token can be used to initiate or manage transaction activity. Tokens can also improve transaction security.

[0030] However, even though tokens provide a certain level of improved transaction security, it is still desirable for a confidence level or risk assessment to be associated with a token because it may reduce the risk of a fraudulent transaction. The confidence level or risk assessment can be referred to as a token assurance level.

Essentially, the token assurance level provides a certain level of “assurance” that the user using the token is in fact the genuine cardholder.

[0031] In some embodiments, the token assurance level is based on how the cardholder, card credential, and/or the token have been authenticated by a payment processing network, an issuer, a merchant, or any other entity in a payment system that is involved in a payment transaction. In some embodiments, the token assurance level may indicate that no authentication has occurred with respect to the cardholder, card credential, and/or the token.

[0032] In some embodiments, the token assurance level may be used for additional risk assessment by the payment processing network and/or issuer prior to approving a payment transaction.

[0033] In some embodiments, determination of the token assurance level can be done at the time of the token request. In other embodiments, determination of the token assurance level can be after generation of the token in response to a token request.

[0034] In some embodiments, the token assurance level can be represented by a token assurance level code within an authorization request message and/or an authorization response message.

[0035] In some embodiments, liability and dispute processing for token payment transactions may be tied to the token assurance level. For example, an entity may bear the liability for a transaction if the token assurance level is low and the entity approves the transaction which ends up being a fraudulent transaction.

[0036] In some embodiments of the invention, token assurance levels may be used in various transactions that use various presentment modes (e.g., QR[™] Code, contactless, remote e-commerce, proximity e-commerce, etc.) for submitting a token as part of a transaction.

[0037] In embodiments of the invention, an entity (e.g., third party wallets, issuers, payment service providers, payment enablers, etc.) can register with the network token system to request a token requestor identifier. The network token

system can store the token to PAN relationship and the token requestor relationship in a token vault. The registered entity can provide their respective token requestor identifier with a token request to the network token system to use its services. For example, the token requestor can request the issuance of a token via API (Application Programming Interface) messaging or a batch request. The network token system can identify and validate the requesting entity based on the token requestor identifier before responding to the token request. Additionally, the network token system can determine a token assurance level to be associated with the token prior to responding to the token request.

[0038] In embodiments of the invention, token request messages may allow a token requestor to request a token to thereby tokenize a PAN. After the token is received by the token requester, the token may be provided to a merchant to conduct a payment transaction. The token may then be subsequently provided to an acquirer, payment processing network, and/or an issuer in an authorization request message and/or clearing messages. In some cases, the token may be replaced by a real PAN before an authorization or clearing message is received by an issuer.

[0039] Some embodiments of the invention can provide an assurance level for a token in a transaction. The token assurance level may indicate a trust level of the token to PAN/consumer binding. In some embodiments, a token assurance level can be determined based on a type of identification and verification process performed and the entity that performed the identity and verification process. For example, the network token system can determine a token assurance level based on the authentication of the consumer, payment account credentials and the token by executing one or more authentication methods. The authentication process can be performed by a payment network and can be network authenticated or can be performed by an issuer to be issuer authenticated. The token assurance level may be determined when issuing a token and may be updated if additional identity and verification processes are performed.

[0040] Using embodiments of the invention, consumers and issuers may benefit from new and more secure ways to pay and improved approval levels. Since token

assurance levels can be associated with tokens, the risk of fraudulent transactions using tokens is greatly reduced. By determining a token assurance level and generating a token assurance code, the probability of the validity and/or authenticity of the token can be determined before a transaction is conducted, thus dispensing with the need to perform fraud and/or verification checking during a payment process. Because the authentication and verification of the token and user of the token has occurred prior to the transaction, embodiments of the invention also have the technical advantage of faster processing during the transaction. This is because additional authentication and verification steps need not be performed.

[0041] Prior to discussing embodiments of the invention, descriptions of some terms may be helpful in understanding embodiments of the invention.

[0042] A “token” may include any identifier for a payment account that is a substitute for an account identifier. 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 primary account identifier or primary account number (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 computationally 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.

[0043] In some embodiments, the token format may allow entities in the payment system to identify the issuer associated with the token. For example, the format of the token may include a token issuer identifier that allows an entity to identify an issuer. For

instance, the token issuer identifier may be associated with an issuer's BIN of the underlying PAN in order to support the existing payment flow. The token issuer identifier may be a different number than the issuer's BIN and may be static. For example, if the issuer's BIN for an issuer is 412345, the token issuer identifier may be 528325 and this number may be static for all tokens issued from or for that issuer. In some embodiments, the token issuer identifier range (e.g., issuer BIN range) may have the same attributes as the associated issuer card range and can be included in an issuer identifier routing table (e.g., BIN routing table). The issuer identifier routing table may be provided to the relevant entities in the payment system (e.g., merchants and acquirers).

[0044] In some embodiments, a token issuer identifier range (e.g., token BIN range) may be 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) associated with issuing tokens. For example, in some embodiments, one or more token BIN ranges can be allocated to each issuer BIN/card range that is associated with an issuer per card volumes for that range. In some embodiments, the token BIN range and allocation can have the same format and definition of the existing BIN routing table format used by relevant entities in the payment processing system. 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. As such, the non-payment tokens may comprise different token issuer identifiers or may not comprise token issuer identifiers. 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 with the payment system.

[0045] "Provisioning" may include a process of providing data for use. For example, provisioning may include providing, delivering, or enabling a token on a device. Provisioning may be completed by any entity within or external to the transaction system. For example, in some embodiments, tokens may be provisioned by an issuer or a payment processing network onto a mobile device. The provisioned tokens may have corresponding token data stored and maintained in a token vault or

token registry. In some embodiments, a token vault or token registry may generate a token that may then be provisioned or delivered to a device. In some embodiments, an issuer may specify a token range from which token generation and provisioning can occur. Further, in some embodiments, an issuer may generate and notify a token vault of a token.

[0046] "Token attributes" may include any feature or information about a token. For example, token attributes may include any 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, token attributes may determine how a token may be used in place of a real account identifier (e.g., PAN) for a transaction. For example, the token attributes may include a type of token, frequency of use, token expiration date and/or expiration time, a number of associated tokens, a transaction lifecycle expiration date, and any additional information that may be relevant to any entity within a transaction processing system. 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 generation of tokens. In some embodiments, a network token system, payment processing 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.

[0047] A type of token may include any information or indicator of how a token may be used. For example, a type of token may be "payment" or "non-payment" to identify the token as being a payment token or a non-payment token. A payment token may include a high value token that can be used in place of a real account identifier (e.g., PAN) to generate original and/or subsequent transactions for a consumer account and/or card.

[0048] Another token type may be a "static" or "dynamic" token type for static and dynamic tokens, respectively. For example, a static token may include a token that may

be issued by a payment processing network or issuer that may be issued in place of an account identifier (e.g., PAN) and may be used for the duration of the underlying account identifier (e.g., PAN). As such, static tokens may be used to submit any number of transactions and may not change for each transaction. Static tokens may be securely stored on the consumer device (e.g., stored in a secure memory or secure element of a mobile device) or in the cloud by the token requestor and may be delivered securely to a mobile device. However, static tokens may include sensitive information that may be protected as they may be used to perform multiple transactions over long periods of time.

[0049] Alternatively, dynamic tokens can include tokens that are limited or restricted in use (e.g., limited by time, amount threshold (aggregated amount or single-transaction amount), or by number of uses). As such, dynamic tokens can be generated and delivered on a per-transaction or on an as needed basis to the end user to initiate a payment transaction through a registered and authenticated device and/or channel. For example, a one-time use dynamic token can be used at electronic-commerce (e-commerce) websites and if the dynamic token is intercepted by a third party, the dynamic token may be useless because it has been used and is thus worthless for future transactions.

[0050] Non-payment tokens may include tokens which are not substitutes for real account identifiers (e.g., PANs). For example, non-payment tokens may be used by merchant/acquirer systems for analytics, offers, customer support, marketing, etc. However, non-payment tokens may not be used to generate original and subsequent transactions using real account identifiers (e.g., PANs) or other account identifiers. Accordingly, non-payment tokens may include low value tokens that may be used for non-payment transactions or transaction services by an entity within the transaction processing system.

[0051] A “frequency of use” of a token may indicate how many times a token can be used in a transaction. For example, a frequency of use may indicate how many times a token may successfully be used in a payment transaction. For example, a

token may include a frequency of use of single-use or multiple-use. A single-use token may be used to generate one transaction. After the first-use of the single-use token, any subsequent use for initiating a transaction can be deemed invalid and a subsequent transaction may be denied. A multi-use token can be used to initiate multiple transactions.

[0052] A “real account identifier” may include an original account identifier associated with a 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 (BIN) that may identify an issuer associated with the real account identifier.

[0053] A “payment token issuer identifier” may include any series of characters, numbers, or other identifiers that may be used to identify an issuer associated with a payment token. For example, a payment token issuer identifier may include a token BIN that identifies a particular issuer associated with an account identified using the token. 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").

[0054] 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., QR™ code, bar code, 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 a 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.

[0055] "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 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).

[0056] "Token exchange" or "de-tokenization" is a process of restoring the data that was substituted during tokenization. For example, a token exchange may include

replacing a payment token with an associated primary account number (PAN) that was associated with the payment token during tokenization of the PAN. 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).

[0057] “Authentication” is a process by which the credential of an endpoint (including but not limited to applications, people, devices, processes, and systems) can be verified to ensure that the endpoint is who they are declared to be.

[0058] An “original” transaction may include any transaction including an authorization provided by an issuer or an authorization provided on-behalf-of an issuer.

[0059] A “substitute” transaction may be any transaction that is associated with an original transaction and that takes place after the original transaction, including repeat, refunds, reversals or exceptions (chargebacks, re-presentments, etc.).

[0060] A “requestor” may be an application, a device, a process, or a system that is configured to perform actions associated with tokens. For example, a requestor can request registration with a network token system, request token generation, token activation, token de-activation, token exchange, other token life-cycle 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). Some non-limiting examples of a requestor may include third party wallet providers, issuers, acquirers, merchants, and/or payment processing networks. A requestor may be referred to as a token requestor when requesting generation of a new token or requesting a new use of an existing token from a network token system. In some embodiments, a token requestor can request tokens for multiple domains and/or channels. Token requestors may include, for example, consumers, card-on-file merchants, acquirers, acquirer processors, and payment gateways acting on behalf of merchants, payment enables

(e.g., original equipment manufacturers, mobile network operators, etc.), digital wallet providers, and/or card issuers.

[0061] A “token requestor identifier” may include any characters, numerals, or other identifiers associated with an entity associated with a network token system. For example, a token requestor identifier may be associated with an entity that is registered with the network token system. In some embodiments, a unique token requestor identifier may be assigned for each domain for a token request associated with the same token requestor. For example, a token requestor identifier 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 identifier may include any format or type of information. For example, in one embodiment, the token requestor identifier may include a numerical value such as a ten digit or an eleven digit number (e.g., 4678012345). In some embodiments, a token requestor identifier 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.).

[0062] An “end-user” may include any application, device, consumer, or system that is configured to interact with a requestor for tokenization/de-tokenization/token management services. For example, an end-user may include a consumer, a merchant, a mobile device, or any other suitable entity that may be associated with a requestor in the network token system.

[0063] 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, accountholder, or user.

[0064] A “card-on-file (COF)” holder may include any entities that store account details (e.g., card details, payment account identifiers, PANs, etc.) for use in transactions. For example, a COF entity may store payment information on file for various types of periodic payments such as monthly utility payments, periodic shopping

transactions, or any other periodic or future transaction. Because payment credentials and/or associated tokens are stored at an entity for a future transaction, the transactions initiated by a COF entity include card-not-present (CNP) transactions. Another type of card-not-present (CNP) transaction includes e-commerce or electronic commerce transactions that are initiated between remote parties (e.g., a consumer device and a merchant web server computer).

[0065] An “authorization request message” may be an electronic message that is sent to a payment processing network and/or an issuer of a payment account 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 a payment account. In some embodiments of the invention, an authorization request message may include a payment token, an expiration date, a token presentment mode, a token requestor identifier, an application cryptogram, and an assurance level data. The payment token may include a payment token issuer identifier that may be a substitute for a real issuer identifier for an issuer. For example, the real issuer identifier may be part of a BIN range associated with the issuer. 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), 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, etc., as well as any other information that may be utilized in determining whether to identify and/or authorize a transaction.

[0066] 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 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 terminal) 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.

[0067] A “server computer” may typically be 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. The server computer may be associated with an entity such as a payment processing network, a wallet provider, a merchant, an authentication cloud, an acquirer or an issuer.

I. EXEMPLARY NETWORK TOKEN PROCESSING SYSTEMS

[0068] FIG. 1 shows a block diagram of a typical transaction processing system 100 configured to use real issuer identifiers (e.g., bank identification numbers (BINs)) to route authorization request messages during transaction processing. For example, payment credentials issued for consumers may include real issuer identifiers (e.g., BINs) that may be used to identify the issuer (and payment processing network) associated with the account being used to initiate the transaction.

[0069] The system 100 may include a consumer 110, a consumer device 120, an access device 130, a merchant computer 140, an acquirer computer 150, a payment processing network computer 160 and an issuer computer 170. In some implementations, different entities in FIG. 1 may communicate with each other using one or more communication networks such as the Internet, a cellular network, a TCP/IP network or any other suitable communication network. Note that one or more entities in the system 100 may be associated with a computer apparatus that may be implemented using some of the components as described with reference to FIG. 11.

[0070] The consumer 110 may be a person or an individual. The consumer 110 may utilize the consumer device 120 to initiate a transaction with a merchant by interacting with the access device 130 (e.g. point-of-sale (POS) device).

[0071] The consumer device 120 may be associated with a payment account of the consumer 110. In some implementations, the consumer device 120 may be a mobile device such as a mobile phone, a tablet, a PDA, a notebook, a key fob or any suitable mobile device. For example, the consumer device 120 may include a wallet or a payment application that may be associated with one or more payment accounts of the consumer 110. In some implementations, the consumer device 120 may be configured to display a machine readable code (e.g., QR[™] code, bar code, etc.). The consumer device 120 may also include a camera or a scanning device capable of scanning a machine readable code. In some implementations, the consumer device 120 may be capable of communicating with the access device 130 using a short range communication technology such as NFC. For example, the consumer 110 may interact with the access device 130 by tapping or waving the consumer device 120 in proximity of the access device 130. In some implementations, the consumer device 120 may be a payment card such as a credit card, debit card, prepaid card, loyalty card, gift card, etc.

[0072] The access device 130 may be an access point to a transaction processing system that may comprise the acquirer computer 150, the payment processing network computer 160, and the issuer computer 170. In some implementations, the access device 130 may be associated with or operated by the merchant computer 140. For example, the access device 130 may be a point of sale device that may include a contactless reader, an electronic cash register, a display device, etc. In some implementations, the access device 130 may be configured to display transaction information in a format that may be read by the consumer device 120 (e.g., mobile phone) including a QR[™] code, bar code, or any other information transfer mechanism. In some implementations, the access device 130 may be a personal computer that may be used by the consumer 110 to initiate a transaction with the merchant computer 140 (e.g., an online transaction).

[0073] The merchant computer 140 may be associated with a merchant. In some embodiments, the merchant computer 140 may be associated with a card-on-file (COF) merchant. For example, the card-on-file merchant may store consumer account

information on file (e.g., at a merchant database) for future payment purposes such as various types of periodic payments (e.g., monthly utilities payments). In some implementations, a consumer may register with one or more merchants for card-on-file services. The merchant computer 140 may be configured to generate an authorization request for a transaction initiated by the consumer 110 using the access device 130.

[0074] The acquirer computer 150 may represent a traditional acquirer/acquirer processor. The acquirer is typically a system for an entity (e.g., a bank) that has a business relationship with a particular merchant, a wallet provider or another entity. The acquirer computer 150 may be communicatively coupled to the merchant computer 140 and the payment processing network 160 and may issue and manage a financial account for the merchant. The acquirer computer 150 may be configured to route the authorization request for a transaction to the issuer computer 170 via the payment processing network computer 160 and route an authorization response received via the payment processing network computer 160 to the merchant computer 140.

[0075] The payment processing network computer 160 may be configured to provide authorization services, and clearing and settlement services for payment transactions. The payment processing network computer 160 may include data processing subsystems, wired or wireless networks, including the internet. An example of the payment processing network computer 160 includes VisaNet™, operated by Visa®. 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 Visa Integrated Payments (VIP) system which processes authorization requests and a Base II system which performs clearing and settlement services. The payment processing network computer 160 may include a server computer. In some implementations, the payment processing network computer 160 may forward an authorization request received from the acquirer computer 150 to the issuer computer 170 via a communication channel. The payment processing network computer 160 may further forward an authorization response message received from the issuer computer 170 to the acquirer computer 150.

[0076] The issuer computer 170 may represent an account issuer and/or an issuer processor. Typically, the issuer computer 170 may be associated with a business entity (e.g., a bank) that may have issued an account and/or payment card (e.g., credit account, debit account, etc.) for payment transactions. In some implementations, the business entity (bank) associated with the issuer computer 170 may also function as an acquirer (e.g., the acquirer computer 150).

[0077] FIG. 2 illustrates a transaction processing system 200 utilizing a network token system, according to one embodiment of the invention.

[0078] The system 200 may include a network token system 202 in addition to one or more components of the traditional payment system 100 as shown in FIG. 1. For example, the system 200 may include a consumer 110, a merchant computer 140, an acquirer computer 150, a payment processing network computer 160 and an issuer computer 170. The system 200 may also include token interfaces 208-218 with the network token system 202 including a token requestor interface 208, a merchant token interface 210, an acquirer token interface 212, a payment processing network token interface 214, a network interface 216, and an issuer token interface 218. In some embodiments of the invention, communication amongst different entities of the system 200 may be encrypted. In some embodiments of the invention, different entities in the system 200 may communicate with one another using one or more communication networks such as TCP/IP, cellular network, etc. In one embodiment, a web service environment for the network token system 202 can provide one or more of the communication interfaces with the network token system and may provide services associated with communication including entity authentication, request authorization, message security, etc..

[0079] The consumer 110 may be able to initiate a transaction using a payment account identifier that may be payment card branded such as Visa®, MasterCard®, American Express®, Discover®, etc. In addition, the consumer 110 may utilize the consumer device 120 to initiate a transaction using any suitable transaction channel. Examples of transaction channels include a scan of a mobile device (e.g., using a QR™

code or bar code), a tap of a mobile device to a merchant access device (e.g., near-field communication (NFC) transaction or other contactless/proximity transaction), a click on an input device (e.g., a mouse) of a computer or mobile device in order to initiate an e-commerce transaction (e.g., online transaction), or through any other suitable channel in which a transaction may be initiated and a token may be passed to a merchant computer. For example, in some embodiments, a mobile device may be used to initiate a remote transaction from a mobile device with a token provisioned onto a secure element or other secure memory of a mobile device.

[0080] A token requestor 204 may include an application, a process, a device, or a system that can request a token from the network token system 202. For example, the token requestor 204 can be an issuer, an acquirer, a card-on-file merchant (also referred to as a merchant of record (MOR)), a mobile device (e.g., a wallet application or a payment application installed on the mobile device), a payment enabler, a payment service provider (PSP), a digital wallet provider (also referred to as a mobile wallet provider), an operating system (OS) provider, a telecommunications network provider, or any other entity that may be use a token or store a token for a third party. The token requestor 204 may interact with the network token system 202 using a token requestor interface 208 for the generation, use and management of tokens.

[0081] In one embodiment, each token requestor 204 may have to undergo an onboarding or registration process to ensure that the token requestor meets integration and security standards in order to use the tokenization services provided by the network token system 202. For example, the network token system 202 may provide services such as card registration, token generation, token issuance, token authentication and activation, token exchange, and token life-cycle management to the registered entities.

[0082] As part of the onboarding process, the token requestor 204 may register with the network token system 202 and may receive a token requestor identifier provided by the network token system 202. The token requestor 204 may specify configuration preferences or token attributes associated with tokens requested by the token requestor including, for example, token type (e.g., static or dynamic), supported

token presentment modes (e.g., scan, contactless, e-commerce, etc.) and any other relevant token configuration information during the onboarding process. Further, the token requestor 204 may include limitations to certain channels (e.g., card-on-file, contactless, etc.) for use of requested tokens.

[0083] The token processing server computer 202B may generate a unique token requestor identifier for each registered token requestor. Thereafter, the registered token requestor 204 can provide the token requestor identifier as part of every network token service request to the network token system 202 as a form of identification.

[0084] The network token system 202 can provide registration for each entity that interacts with the network token system.

[0085] The token requestor 204 may be configured to request a new token or request life-cycle management actions for an existing token (e.g., change an existing token, deactivate a token, etc.). In some embodiments, a token requestor 204 may provide an account identifier (e.g., a PAN) and an expiration date with a request for a new token. The network token system 202 may use the token requestor identifier to identify and validate the token requestor 204 as well as validate a token based transaction when processing a transaction initiated using a token.

[0086] The network token system 202 may include a token registry database 202A and a token processing server computer 202B. The token registry database 202A may also be referred to as a “token vault.” The token registry database 202A may store and maintain issued or generated tokens as well as any other relevant information to the tokens. For example, the token registry may include a token requestor identifier and an account identifier (e.g., PAN) for each token. The token registry database 202A and the token processing computer 202B may be configured to provide services associated with the token registry including, for example, payment account registration, token generation, token issuance, token authentication and activation, token exchange, token routing, token assurance level generation, token lifecycle management, and token processing to the entities that are registered with the network token system 202. In some embodiments, different entities can communicate with and obtain services

provided by the network token system 202 using their respective interfaces with the network token system 202.

[0087] Tokens in the token registry database 202A may include different token states that may determine whether a token may be used in a transaction as well as the actions necessary to allow a token to be used in a transaction. For example, token states may include active, inactive, suspended, on hold, deactivated, or any other indication of the availability for a token to be used in a transaction. For instance, in some embodiments, a token may be generated by the token vault and may be immediately active and available for transacting. Further, issuers may notify the payment processing network computer 160 or the network token processing server computer of tokens that are “inactive” or not currently in use. In some embodiments, the token value associated with an inactive token may be treated in the same manner as “not found,” by a token processing server computer. A token may be changed to “suspended” which includes a temporary state in which no authorizations or full financial original transactions can be performed with the token. A “deactivated” token status may include a token that may be permanently suspended and no authorizations or full financial original transactions may be performed. In some embodiments, tokens may reflect certain attributes relevant to the account identifier (e.g., PAN) being tokenized. For example, in some embodiments, the token may reflect funding source and the country associated with the underlying account identifier.

[0088] In some embodiments, the merchant computer 140 and the acquirer computer 150 may be provided with a token in lieu of a real account identifier (e.g., PAN) for various transaction use cases. For example, the merchant computer 140 and/or acquirer computer 150 may receive a token in the traditional PAN field of authorization request message and may forward the authorization request message to the payment processing network computer 160 for processing. The payment processing network computer 160 may replace the token with the real account identifier (e.g., PAN) and send a modified authorization request message to the issuer computer 170. In some embodiments, the authorization request message may further have the token moved to a new field in the authorization message and/or clearing message for

the issuer computer 170 to receive so that the issuer may receive both the account identifier (e.g., PAN) and the token in such messages.

[0089] Accordingly, in some embodiments, the issuer computer 170 may be configured to receive both the real account identifier (e.g., PAN) and the token in the authorization request messages and in transaction clearing messages received from the payment processing network computer 160. Chargebacks and chargeback reversal messages may also contain both the token and the real account identifier (e.g., PAN). In some embodiments, the issuer computer 170 may choose to have the payment processing network computer 160 call out to have the issuer computer 170 provision the tokens. In some embodiments, the issuer computer 170 may provide the payment processing network computer 160 with its current token database via a bulk file interface.

[0090] In some embodiments, the token requestor interface 208 may be used by the token requestor 204 to interact with the network token system 202. For example, the token requestor 204 may send requests for multiple actions including token issuance, token lifecycle management (e.g., activation, deactivation, account credential update, etc.), and token authentication. In some embodiments, the token requestor interface 208 may include an application programming interface (API) or any other relevant messaging formats may be used. For example, the token requestor 204 may send a token issuance request that includes account information (e.g., a PAN and any other account details) and a token requestor identifier. Additionally, in some embodiments, the token requestor 204 may provide a bulk token request file that includes a plurality of account identifiers (e.g., PANs) and a token requestor identifier. The network token system 202 may generate and return a plurality of tokens, where each token is associated with an account identifier (e.g., PAN) from the bulk file request. In some embodiments, the token requestor 204 may optionally provide one or more token attributes with the request such as, for example, a frequency of use (e.g., single-use or multi-use), a type of token (e.g., payment or non-payment), a token expiration date and/or time, a number of requested tokens, a transaction lifecycle expiration date, etc. In some embodiments, the token request may further include one or more of an

MSISDN (Mobile Subscriber Integrated Services Digital Network-Number), an account nickname (e.g., an alias), a UUID (Universally Unique Identifier) associated with the account or consumer, an IMEI (International Mobile Station Equipment Identity), an IMSI (International Mobile Subscriber Identity), a mobile application identifier, a purchase amount, etc. Additionally, in some embodiments, merchants can use the token requestor interface 208 to request for non-payment tokens (e.g., to use in analytics, loyalty, rewards, or any other business related processes).

[0091] Further, a token requestor 204 may request that the network token system 202 add a token to the account identifier (e.g., PAN) relationship to the token registry database 202A. The token requestor 204 may also request that the network token system 202 change the attributes for a token to account identifier (e.g., PAN) relationship in the token registry database 202A. For example, the token requestor 204 may request that the network token system 202 suspend a token due to the loss of a device by the consumer. The token requestor 204 may request that the network token system 202 deactivate a token in the token registry database 202A. In some embodiments, the corresponding record in the token registry database 202A may be marked deactivated (e.g., no longer valid for new purchases), but may remain available for exception processing for a limited period of time and may then be subsequently removed. In some embodiments, the network token system 202 may purge the tokens that have expired or that have been deactivated for a period of time on a periodic basis. Token requestors may also create batch files of token requests (e.g., add, delete or deactivate) and send them to the network token system 202 on a periodic basis.

[0092] In some embodiments, the token vault may comprise the following records.

Element	Description
Token	A token may be an identifier or a key. In embodiments of the invention, one or more tokens may be mapped to a PAN. A token may include a numerical value, e.g., a

	sixteen, eighteen, or a nineteen digit number.
PAN	A PAN may be a primary account number mapped to one or more tokens. A PAN may include a numerical value, e.g., a sixteen, eighteen, or nineteen digit number.
User BID	A user business identifier may be associated with an issuer associated with the PAN. The user BID may be used to facilitate maintenance and tracking. A user BID may include an six, seven, or eight digit numerical value.
Token Type	A token type of indicate the type of token, such as a token specifically used for e-commerce, card-on-file, NFC, etc. transactions. A token type may include an assigned number, e.g., 5 for card-on-file, 2 for NFC, etc.
Allowed MCCs	An MCC may be a merchant category code that can be used for token use. The allowed MCC fields may include any suitable number of values (e.g., up to 24 assigned numbers).
Merchant of Record (MOR)	A merchant of record identifier may identify the merchant. The MOR field may include any suitable number of values (e.g., an 8 digit number).
Token Service	A token service indicator may identify the entity that provides the token service. It may identify a payment processing network if the token service was provided by the payment processing network or the payment processing network on behalf of the issuer. The token service field may include an assigned number, e.g., 1 for on behalf of the issuer.

Token Class	A token class indicator may indicate that the token is assigned to a payment processing network token range or issuer assigned range. The token class field may include an assigned number, e.g., 1 for issuer.
Token Expiration Date	The token expiration date may refer to the expiration date of the token. The token expiration date can be equal to or less than the PAN expiration date. If expired, the token may be unusable. The token expiration date may be updated by a token requestor, an issuer, or via an internal process run by the network token system 202. The token expiration date field may include 4 digit unassigned numbers, e.g., 0517 for May 2017.
State of Token	The state of token indicator may indicate whether the token is active or deactivated. If it is deactivated, it may be valid only for exception transactions. It may be updated through token requestor change records. The state of token field may include an assigned number, e.g., 1 for active, 2 for de-activated, etc.
Deactivation Date	The deactivation date indicator may indicate the deactivation date for the token. It may be updated through the token requestor change records. The deactivation date field may include any number of digits including a 4 digit unassigned number, e.g., 0314 for March 2014.
Token Requestor Identifier	A token requester identifier may identify a token requestor. The token requester identifier may restrict the token use to the token requestor associated with this identifier. A token requester identifier in the token

	registry database 202A may be matched with a token requestor identifier in an authorization request message in a transaction. The token requestor identifier field may hold any suitable number of digits, including a 11 digit number, e.g., 45590790789.
Token Assurance Level	A token assurance level indicator may include a level of authentication assurance at the time of token issuance. It may be updated through the token requestor change records. The token assurance level field may include any suitable number of digits including a 2 digit assigned number, e.g., 25.
Purge Date	A purge date indicator may indicate a date on which the token is to be entirely removed from the token vault. The purge date field may include any suitable number of digits including a 4 digit unassigned number, e.g., 0814 for August 2014.

[0093] In some embodiments of the invention, for NFC token requests, a token requestor identifier, a real account identifier (e.g., PAN), a token expiration date and a token assurance level may be stored in the token vault for each token entry.

[0094] For card-on-file e-commerce merchant requests, the token requestor interface 208 may be used by the token requestor 204 to interact with the network token system 202. For example, the token request may include whether the request is for a new token, change of an existing token, or deactivation of a token. The token requestor 204 may also provide a token requestor identifier, a PAN, an expiration date, a token type with the token request. In one embodiment, the AVS and CAVV data presented for the identity and verification process may only be used for authentication and is not stored in the token vault.

[0095] The network token system 202 may generate a token that has the same format as a PAN to minimize disruption across the payment system and has a value that does not collide with any real PAN or an active token. In some embodiments, if a token has not been used in an authorization request by the intended expiration date/time, the token may be reissued by the network token system 202.

[0096] In some embodiments, the network token system 202 may provide token lifecycle management services to the registered entities. Lifecycle management can be useful when a token is compromised or a payment device is lost. For example, the network token system 202 may de-activate a token and its associations when the token becomes inactive, suspended or temporarily locked. The network token system 202 may deactivate a token by temporarily locking or suspending the token for a specific token requestor. The network token system 202 may also cancel a token to permanently mark a token as deleted to prevent any future transactions. A deleted token can be used during returns/chargebacks if the same token was used to submit the corresponding original transaction for a specific token requestor. The network token system 202 may also update token attributes such as token validity timeframes (e.g., extend or reduce the timeframe) or frequencies of permitted token use. The token validity timeframe can refer to a specific number of days, hours, minutes, or a specific expiration date.

[0097] In some embodiments, the network token system 202 may allow the registered entities to allow the consumers to update information about the PAN, e.g., assign a different PAN to a static token. For example, the entity may provide a token requestor identifier, an old PAN and a new PAN to the network token system 202 using its interface. The network token system 202 may generate a new static token and associate it to the new PAN. The old token association could then be deactivated.

[0098] In some embodiments, the network token system 202 may support tokens generated by other entities such as issuers or wallet provider systems. For example, the token registry database 202A may be configured to store the PAN and token

mapping and any other attributes for external tokens. The entities can provide the external tokens using their respective interfaces with the network token system 202.

[0099] In some embodiments, the network token system 202 may allow the registered entities to request CVV2 (Card Verification Value) values (or other types of verification values, cryptograms, etc.) for tokens using their respective interfaces. The network token system 202 may use the token to determine the real account identifier (e.g., a PAN) and can communicate with the payment processing network computer 160 (e.g., using an API) to request CVV2 values associated with the real account identifiers. These CVV2 values may be provided to the requesting entities.

[0100] In some embodiments of the invention, the network token system 202 may allow the registered entities to provide details of the transactions submitted using tokens using their respective interfaces. For example, a registered entity may provide a token requestor identifier, a transaction identifier, a transaction amount, a transaction date and time, a merchant identifier, a merchant address, an MSISDN, a UUID, an IMEI, etc. This data may be stored in the token registry database 202A. These details may be used for loyalty or other types of programs. For example, the transaction details can be used to identify relevant offers that might be of interest to the consumers conducting the transactions.

[0101] In some embodiments, the network token system 202 may allow the registered entities to request transactions made using tokens by providing the token requestor identifier, a token or token alias, and a date range (e.g., start and end date). The network token system 202 may provide a list of transactions conducted with the token or the alias within the identified date range.

[0102] In some embodiments, the network token system 202 may allow the registered entities to request authorization and settlement data for a given token/PAN combination and date range by providing a token requestor identifier, a PAN, a token and a date range.

[0103] In some embodiments, the network token system 202 may allow the registered entities to request all the tokens and their attributes assigned for a given PAN and a date range by providing a token requestor identifier, a PAN and a date range.

[0104] In some embodiments, the network token system 202 may allow the registered entities to request details for a specific token and PAN combination by providing a token requestor identifier, a PAN and a date range.

[0105] In some embodiments, the network token system 202 may provide an interface for e-commerce merchants to integrate into their web applications to initiate token generation requests for card-on-file transactions during checkout processes. For example, e-commerce merchants may provide a token requestor identifier, a PAN (card-on-file), a CVV2, an expiration date and optionally a consumer user identifier used for an e-commerce web application using the merchant token interface 210. The network token system 202 may provide in return a token and dCVV to the merchant computer 140. The token and the dCVV may be validated by the payment processing network computer 160 when it is received from the merchant computer in an authorization request message during a payment transaction.

[0106] In some embodiments, the network token system 202 may provide an interface for e-commerce merchants to provide an option for the consumers to request a token during checkout to use in place of a PAN. For example, the e-commerce merchants may provide a token requestor identifier, a PAN (card-on-file), a CVV2, an expiration date and optionally the consumer's first and last name, and billing address using the merchant token interface 210. The network token system 202 may authenticate the consumer/PAN before generating a token. The network token system 202 may provide a token and dCVV to the merchant computer. The token and the dCVV may be validated by the payment processing network computer 160 when it is received from the merchant computer in an authorization request message during a payment transaction.

[0107] In some embodiments, the network token system 202 may provide a user interface for the consumer 110. The user interface may allow the consumer to perform

operations such user registration, payment account registration, token request generation, token deactivation, etc. In some embodiments, the network token system 202 may authenticate the consumer 110 and/or the PAN before generating and supplying a token to the consumer 110.

[0108] In some embodiments, the network token system 202 may provide a notification advice message to notify participating issuers or other entities that one of their consumers has requested a token (e.g., requested that their phone be provisioned with a token) using the network token system provisioning service. The advice message may include a message reason code (e.g., token create, token deactivate, token suspend or token resume), a token number, a token assurance level and a token requestor identifier.

[0109] In some embodiments, the merchant token interface 210 may allow the merchant computer 140 to communicate with the network token system 202 for tokenization and de-tokenization services such as token exchange, token processing and routing, etc. In some embodiments, the merchant token interface 210 may include an API. For example, the merchant computer 140 may use the merchant token interface 210 to request PAN information associated with a given token from the network token system 202 by providing a token requestor identifier, a token value and a date (e.g., transaction date or date range). In some embodiments, de-tokenization of a token may be requested during authorization and clearing process for a transaction. In some embodiments, the token exchange may be requested for bulk tokens.

[0110] In some embodiments, the acquirer token interface 212 (which may be in the form of an API) may allow the acquirer computer 150 to communicate with the network token system 202 for tokenization and de-tokenization services. Tokenization and de-tokenization services may include token exchange, token processing and routing, etc. For example, using the acquirer token interface 212, the acquirers may request that the network token system 202 provision a token on their behalf. A merchant, acquirer or a wallet provider may receive the token in response to a provisioning request message originating from an acquirer. The provisioning request

message may support card-on-file provisioning and NFC provisioning. For example, the provisioning request message may include a PAN, a transaction amount, a transaction date and time, an expiration date, a merchant type, an acquirer's country code, a POS entry mode code (e.g., manual key entry, contactless device read, etc.), an acquirer's identifier code, an AVS result code, a CVV2 result code, a CAVV result code, CAV data, and any other relevant data.

[0111] In other embodiments, the acquirer computer 150 may use the acquirer token interface 212 to request PAN information associated with a given token from the network token system 202. This can be accomplished by providing the token along with a token requestor identifier, a token value and a date (e.g., transaction date or date range) to the acquirer token interface 212. In some embodiments, de-tokenization of a token may be requested during authorization and clearing process for a transaction via the acquirer token interface 212. In some embodiments, a token exchange process for bulk tokens can be conducted through the acquirer token interface 212.

[0112] In some embodiments, the payment processing network token interface 214 may allow the payment processing network computer 160 to communicate with the network token system 202 for tokenization and de-tokenization services such as token exchange, token processing and routing, etc. For example, the payment processing network computer 160 may provide a token to the network token system 202 in exchange for a PAN or vice-versa.

[0113] In some embodiments, network interface 216 may allow a gateway or other networks 206 (e.g., MasterCard®, American Express®, Discover®, etc.) to communicate with the network token system 202 for tokenization and de-tokenization services via the payment processing network computer 160, e.g., token exchange, token routing, etc. For example, the other networks 206 may interact with the network token system 202 or the issuer computer 170 for the exchange of a token with a PAN for transactions initiated using debit card accounts.

[0114] In some embodiments, the issuer token interface 218 may allow the issuer computer 170 to communicate with the network token system 202 for tokenization and

de-tokenization services, e.g., token registration, token authentication, etc. In some embodiments, the participating issuers may request that the network token system 202 tokenize PANs and manage existing tokens. For example, the issuer computer 170 may provide a request via the issuer token interface 218 that the network token system 202 create a token, deactivate a token, suspend a token, or resume a token. Further, the issuer token interface may allow an issuer to perform a token inquiry, update an account identifier (e.g., PAN) expiration date, replace an account identifier (e.g., a PAN) associated with a token, or update card art or other information associated with a token (e.g., terms and conditions, etc.). Additionally, the token processing server computer 202B may provide notifications and other information through the issuer token interface 218. For example, the notifications may include token creation notifications, device provisioning notifications, authentication results, and deactivate, suspension, and resuming token notifications.

[0115] In some embodiments, an issuer may generate and provide tokens to the network token system. For example, an issuer may provide the token to the payment processing network computer 160 to store in the token vault on the issuer's behalf. For example, the issuer computer 170 may provide information such as an account identifier (e.g., PAN), a token, a token assurance level, a token requestor identifier, a token expiration date, a token type, and a state of the token to the token processing server computer 202B. The token processing server computer may validate that there is no conflict with the token (i.e., that a token already exists for that value) and may generate a token entry associated with the provided token information in the token registry database 202A.

[0116] Additionally, in some embodiments, the issuer computer 170 may request that the payment processing network 160 generate tokens using an issuer's own account range, and not the payment processing network's token range. If the issuer token range does not conflict with another token or account issuer identifier range that is already in use, the token processing server computer 202B may generate an association or linkage between the issuer's token account range and the issuer's real issuer identifier (e.g., BIN) range. In some embodiments, the issuer token interface 218

may allow the issuers to submit bulk registration file containing the tokens generated by the issuer. In some embodiments, if the issuer computer 170 fails to respond to a token request (for individual or bulk requests) in the instances of issuer token provisioning, then the token request to the token requestor 204 may be declined. For example, the token requestor 204 may receive a notification informing the token requester that an issuer timeout has occurred.

[0117] FIG. 3 illustrates components of the token processing server computer 202B in one embodiment of the invention.

[0118] The token processing server computer 202B may include a processor 300 communicatively coupled to a network interface 302, a memory 304 and a computer readable medium 306.

[0119] The processor can comprise a CPU, which comprises at least one high-speed data processor adequate to execute program components for executing user and/or system-generated requests. The CPU may be a microprocessor such as AMD's Athlon, Duron and/or Opteron; IBM and/or Motorola's PowerPC; IBM's and Sony's Cell processor; Intel's Celeron, Itanium, Pentium, Xeon, and/or XScale; and/or the like processor(s). The CPU interacts with memory through signal passing through conductive conduits to execute stored signal program code according to conventional data processing techniques.

[0120] The network interface 302 may be configured to allow the network token system 202 to communicate with other entities such as the consumer device 120, merchant computer 140, acquirer computer 150, payment processing network computer 160, issuer computer 170, etc. using one or more communications networks. Network interfaces may accept, communicate, and/or connect to a communications network. Network interfaces may employ connection protocols such as, but not limited to: direct connect, Ethernet (thick, thin, twisted pair 10/100/1000 Base T, and/or the like), Token Ring, wireless connection such as IEEE 802.11a-x, and/or the like. A 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.

[0121] The memory 304 may be used to store data. The memory 304 may be coupled to the processor 300 internally or externally (e.g., cloud based data storage) and may comprise any combination of volatile and/or non-volatile memory, for example, RAM, DRAM, ROM, flash, or any other suitable memory device.

[0122] The computer readable medium 306 may be in the form of a memory (e.g., flash, ROM, etc.) and may comprise code, executable by the processor 300 for implementing methods described herein. The computer readable medium 306 may include a requestor registration module 308, a card registration module 310, a token generation module 312, a verification and authentication module 314, a token exchange and routing module 316, a token life-cycle management module 318 and, a reporting and administration module 320. The computer readable medium 306 may also comprise code, executable by the processor 300 to implement a method comprising: receiving a first token request message from a first entity; analyzing the first token request message; determining the first token request message includes a request for a token; determining a first token; transmitting the first token to the first entity; receiving a second token request message from a second entity; analyzing the second token request message; determining the second token request message includes a token request associated with the first token; determining token attributes associated with the first token; and transmitting the determined token attributes to the second entity. The computer readable medium 306 may also comprise the computer readable medium comprising code, executable by the processor, for implementing a method comprising: generating a token request from a token requester; performing at least one authentication process associated with the token request; in response to the performance of the at least one authentication process, generating a token assurance code; and transmitting the token to the token requester

[0123] The requestor registration module 308 may comprise code which can cause the processor 300 to register each token requestor entity with the token registry database 202A and to generate a token requestor identifier for the registered entity. Some non-limiting examples of the token requestor entities may include issuers, wallet providers, payment enablers (e.g., merchant, wallet providers or OEMs having a card-on-file repository), merchants, e-commerce merchants, transit authorities, payment processing networks, acquirers, mobile devices (e.g., wallet application, payment application, etc.), or subcomponents and applications thereof, and consumers. Each registered entity can use the token requestor identifier as part of each token service request with the network token system 202 which can help identify and validate the entity. In one embodiment, the registered application can provide token requestor information to the requestor registration module 308 such as an entity name, contact information, an entity type (e.g., merchant, wallet provider, payment service provider or PSP, issuer, payment enabler, acquirer, acquirer processor, etc.), token presentment modes (e.g., scan, contactless, e-commerce, etc.), token type (e.g., static/dynamic, payment/non-payment), integration and connectivity parameters, and services subscribed (e.g., token request, authentication and verification, life-cycle management, etc.) and any other relevant information for the onboarding process.

[0124] Referring back to FIG. 2, in some embodiments, each token requestor 204 can register with the token registry database 202A using the token requestor interface 208. For example, a graphical user interface may be used to provide token requestor information to the network token system 202. The user interface may be a conventional graphic user interface as provided by, with, and/or atop operating systems and/or operating environments such as Apple Macintosh OS, e.g., Aqua, GNUSTEP, Microsoft Windows (NT/XP), Unix X Windows (KDE, Gnome, and/or the like), mythTV, and/or the like. The user interface may allow for the display, execution, interaction, manipulation, and/or operation of program components and/or system facilities through textual and/or graphical facilities. The user interface provides a facility through which users may affect, interact, and/or operate a computer system.

[0125] The requestor registration module 308 may validate the information and upon successful validation may store the token requestor details in the token registry database 202A. The requestor registration module 308 may also generate a token requestor identifier after successful registration. In one embodiment, the token requestor identifier is a ten digit numerical value. However, other formats of the token requestor identifier are possible. In some embodiments, as part of the registration process, the token registry database 202A may store requestor entity information such as a business identifier, a token requestor identifier, a token requestor type (e.g., payment enabler, merchant of record, merchant, acquirer, issuer, etc.), and a platform type (e.g., a payment enabler mobile application, payment enabler online, merchant application, payment service provider application, issuer wallet application, etc.).

[0126] The card registration module 310 may comprise code that can be used by the processor 300 to perform card registration by different entities. In some embodiments, the network token system 202 may allow the registered entities to register their payment cards or accounts with the network token system 202 using their respective interfaces. For example, the registered entities may provide a token requestor identifier (e.g., received at the time of registration from the requestor registration module 308), a payment account number, a CVV2, an expiration date, consumer name and contact information, a token type, an OS type/version, and any other relevant information for individual card registration or bulk card registration. In one embodiment, the card registration module 310 may store the details of all of the consumers' account details in the token registry database 202A for all successful activation and registration requests. In one embodiment, the token registry database 202A may store a token requestor identifier, a MSISDN, a payment account number, a CVV2, an expiration date, a PAN nickname or alias, a consumer postal code, a UUID, a IMEA, an IMSI, a mobile application identifier, consumer first and last name, etc. In one embodiment, the registered entities may use their respective interfaces to unregister payment accounts by providing the necessary information to network token system 202.

[0127] The token generation module 312 may be configured to generate a token in response to a request for a token from a token requestor. In one embodiment, the

token generation module 312 may receive a token requestor identifier, an account number (e.g., PAN), an expiration date and a CVV2. In some embodiments, the token generation module 312 may also receive optional information such as a consumer name, a consumer address and zip code, a requested token type (e.g., payment static, payment dynamic, non-payment, etc.), a card verification status (e.g., AVS/CVV check status), a MSISDN, a UUID, an IMEI, an OS type/version and any other suitable information. In one embodiment, the token generation module 312 may generate a token response with a token number, a token expiration date and a token assurance level. In one embodiment, the token generation module 312 may validate the token requestor identifier, determine the PAN type and generate a token from the respective token BIN ranges. The token registry database 202A may maintain the correlation between the card and the associated requestor and the token. In one embodiment, the token generation module 312 may determine if a token already exists in the token registry database 202A for the token request before generating a new token. In some embodiments, if a token cannot be provisioned, the token response may include a corresponding reason code. The token generation module 312 may also provide an interface to the token requestors to submit a bulk token request file.

[0128] In one embodiment, the tokens may be generated on-the-fly via API calls (e.g., using the token requestor interface 208). For example, when a request is received to tokenize a PAN, the token generation module 312 may determine a token range to assign the token. For example, the token range may be assigned based on whether the issuer is provisioning the token (e.g., issuer assigned token range) or the payment processing network is provisioning the token on-behalf-of the issuer (e.g., payment processing network assigned token range). As an example, if the payment processing network assigned token range includes “442400000-442400250”, then “4424000000005382” may be assigned as a token value. The token vault may store the relationship of the token range to the PAN and a token add record may be logged. In some embodiments, the token generation module 312 may consider the token range list associated with the PAN range before assigning a token.

[0129] In one embodiment, the token generation module 312 may access a token range table that represents available token ranges provisioned by the payment processing network computer 160 and token ranges have not been associated with PAN ranges. The token generation module 312 may access another table that includes minimum and maximum account ranges for the PAN and the associated token ranges. The token ranges may include the token ranges provisioned by the payment processing network computer 160 and the token ranges provisioned by the issuer computer 170.

[0130] In one embodiment, the merchant token interface 210 may allow the e-commerce merchants to initiate token generation requests for cards-on-file during checkout processes using those cards on file. For example, the token generation module 312 may receive a token requestor identifier, a card-on-file PAN, a CVV2, an expiration date, and optionally a consumer identifier for the e-commerce web application. The token generation module 312 may provide a token and dCVV which may be validated by the payment processing network computer 160 during the authorization process. For example, the token and dCVV may be provided to the merchant computer, which may then generate an authorization request message using the token and dCVV. The payment processing network may then receive the authorization request message and may validate the token and dCVV, or possibly replace the token and dCVV with the real account number and CVV2 value corresponding to the account number.

[0131] In one embodiment, the merchant token interface 210 may allow the e-commerce merchants to provide an option to the consumer 110 to request a token during checkout in place of the PAN. In such embodiments, the token generation module 312 may authenticate the consumer and/or PAN before generating a token. For example, the token generation module 312 may receive a token requestor identifier, a card-on-file PAN, a CVV2, an expiration date, and optionally a consumer name and billing address, and may provide a token and dCVV to the consumer, which may be validated by the token processing server computer 202B during transit. For example, the token and dCVV may be provided to the consumer's computer, which may be provided to the merchant computer, which may then generate an authorization request

message using the token and dCVV. The payment processing network may then receive the authorization request message and may validate the token and dCVV, or possibly replace the token and dCVV with the real account number and CVV2 value corresponding to the account number.

[0132] The verification and authentication module 314 may be configured to execute a consumer verification and authentication process. For example, the verification and authentication module 314 can perform consumer authentication and verification through a configured authentication scheme. In one embodiment, the authentication scheme may include verification of the payment account number, CVV2 and the expiration date based on the customer information stored in a database associated with the payment processing network. In one embodiment, the authentication scheme may include direct verification of the consumer by the issuer computer 170 with consumer credentials for their online banking system.

[0133] In one embodiment, the authentication scheme may include verification of the consumer credentials through the issuer ACS (Access Control Server). For example, the issuer ACS service may be part of an authentication protocol such as 3-D secure protocol by Visa[®]. The ACS server may be associated with the issuer computer 170 that may include registered consumer account and access information. The ACS can give issuers the ability to authenticate consumers during an online purchase, thereby reducing the likelihood of fraudulent use of payment accounts. For example, the ACS can validate that the consumer is registered, performs consumer verification at the time of the transaction and provides digitally signed responses to the merchants. A directory server with the addresses of many ACS computers associated with many issuers may be present in a 3-D Secure type system, and the directory server may route messages to and from the ACSs.

[0134] In one embodiment, the authentication scheme may include verification of the payment account using a payment processing network consumer authentication service (e.g., Visa[™] Consumer Authentication Service (VCAS)). For example, the

VCAS service can authenticate the consumer on-behalf of the issuer prior to the authorization process.

[0135] In some embodiments, the authentication scheme may be based on the use of OTP (One time Password) or zero dollar authorization request message. For example, the OTP may be provided to the consumer 110 by the payment processing network computer 160 or the issuer computer 170. The consumer 110 can utilize the consumer device 120 to provide the OTP to the network token system 202 for authentication. In other embodiments of the invention, a zero dollar authorization request message may be sent by a merchant computer 140 to the issuer computer 170 via the acquire computer 150 and the payment processing network computer 160 to verify the identity of the consumer and/or the validity of a payment account. In one embodiment, a zero dollar transaction (i.e., an authorization request message with a zero dollar amount) may be used to verify the payment account number, any personal identifier (e.g., a PIN), address, and/or verification values (e.g., CVV, CVV2, or other variants, etc.).

[0136] In some embodiments, requests to provision tokens may combine consumer authentication requests with the token request. For example, authentication may be performed prior to tokenization using any of the previously discussed authentication methods. In the authentication methods, where the issuer computer 170 performs the authentication, tokenization may be performed after receiving an authentication response from the issuer computer 170.

[0137] In some embodiments, account or card registration, token generation, and verification and authentication may be performed as part of a single token request process. In some embodiments, for bulk requests, card registration and token generation may be performed by processing a bulk file from the token requestor 204. In such embodiments, consumer verification and authentication may be performed in a separate step. In some embodiments, the token requestor 204 can request that the authentication and verification process be performed independently multiple times for a

particular card or account to reflect any changes to the levels of assurance for the token over time.

[0138] The token exchange and routing module 316 may comprise code, executable by the processor, to cause the processor to allow registered applications to request payment account number information for a given token. For example, the payment processing network 160, acquirer computer 150, etc. may issue a request for a token exchange during a payment transaction. In one embodiment, a registered entity can provide at least one, two or more of a token requestor identifier, a token number, a token expiration date, a token presentment mode, a transaction identifier, a transaction timestamp, a request timestamp and any other relevant information to request the payment account number information. The token exchange and routing module 316 may validate that the requesting entity is entitled to make a request for a token exchange. In one embodiment, the token exchange and routing module 316 may validate the PAN/token mapping and presentment mode based on the request timestamp and the token expiration timestamp. The token exchange and routing module 316 may retrieve the payment account number information from the token registry database 202A and provide it along with the assurance level to the requestor entity. In one embodiment, if the PAN/token mapping is not valid for the requested timestamp and presentment mode, an error message may be provided.

[0139] The token life-cycle management module 318 may comprise code, executable by the processor 300 to perform lifecycle operations. Lifecycle operations may include canceling a token, activating or deactivating a token, updating token attributes, renewing token with a new PAN expiration date, etc. In one embodiment, a token requestor entity may provide a token requestor identifier, a token number, a lifecycle operation identifier and one or more token attributes to the network token system 202 to perform the requested lifecycle operation on the given token. The token life-cycle management module 318 may verify the token requestor identifier and the token association based on the token registry database 202A. The token life-cycle management module 318 may perform the requested lifecycle operation on the given

token number and update all the corresponding association in the token registry database 202A.

[0140] The token requestor 204 request a lifecycle operation using an interface. The lifecycle operation may be associated with a lost or stolen consumer device, a compromised payment account number or the token, a change in the payment account number, unsubscribing a card-on-file, etc. In another example of a lifecycle operation, a token activation operation may be requested to activate an inactive, suspended or temporarily locked token and its associations. A token de-activation operation may be requested to temporarily lock or suspend a token. A cancel token operation may be requested to permanently mark a token and its associations as deleted to prevent any future transactions. In some embodiments, a deleted token may be used during returns/chargebacks if the same token was used to submit the corresponding original transactions. A token update operation may be requested to update token attributes such as expiration date (e.g., extend or reduce the validity timeframe), timestamp, frequency of usage (based on token details provided), etc. Validity timeframe can be number of days/hours/minutes or specific expiration date.

[0141] In some embodiments, the network token system 202 may allow consumers to request update the association between a PAN and a static token. For example, the consumer 110 may request that his PAN be updated. This update can occur through the token requestor interface 208 or the issuer computer 170 may request that the PAN be updated via the issuer token interface 218. The registered entity may provide a token requestor identifier, the old PAN and optionally the new PAN to the token life-cycle management module 318, which can associate the new PAN to the static token or can generate a new static token for the new PAN.

[0142] The reporting and administration module 316 may allow the token requestors to request transaction details made using tokens by providing a token requestor identifier, a token or PAN alias and a transaction date range (e.g. a start and end date). In one embodiment, the network token system 202 may retrieve all the token transactions from the payment processing network 160 and maintain in a data store to

provide the transaction details to the requesting registered entity to handle returns, chargebacks and disputes and to support analytics. The reporting and administration module 316 may provide the transaction details made using the given tokens (or tokens associated to the given PAN alias) between the given date range.

[0143] In some embodiments, the reporting and administration module 316 may allow the registered entities to request authorization and settlement data from a given token/PAN combination and date range. In some embodiments, the reporting and administration module 316 may allow the registered entities to request all the tokens and their attributes assigned for a given PAN and from a given date range.

[0144] The token assurance module 322 may be configured to determine a token assurance level associated with the token generated by the token generation module 312. The token assurance level may be determined based on the outcome of the verification and authentication performed by the verification and authentication module 314. The token assurance level may indicate assurance information associated with the token, such as an assurance indicator (e.g., requestor, network, issuer, ACS, other), an entity that performed the assurance (e.g., requestor, network issuer, others), a date the assurance was performed, a wallet/consumer device identification, an assurance level score (based on authentication method used) and any other relevant information. The token assurance module 322 can determine the token assurance level at the time of the token request, or may determine the token assurance level at a later time. The token assurance level can be used for additional risk assessment by the payment processor network or the issuer.

[0145] In some embodiments, token assurance level may include assurance information such as an assurance indicator, an entity that performed the authentication or assurance process (e.g., requestor, network issuer, others), the date that the assurance processing was performed, a wallet/consumer device identification indicator, an assurance level score (based on authentication method used), and any other information relevant to assurance. Assurance indicators and scores are examples of assurance codes.

[0146] Some examples of the token assurance information include, but are not limited to, an indication that the token has not been authenticated, an indication that the token is network authenticated, an indication that the token is issuer authenticated, or any other indication of how the token, cardholder, and/or card credential was authenticated. The token processing server computer 202B may record the token assurance level once the token vault records the authentication via verification and authentication module 314.

[0147] In some embodiments, the payment processing network 160 may track the token assurance level based on the authentication and request for a token binding. This may be used to inform the issuer that the token has been verified using additional authentication techniques. Further details regarding the token assurance level are described below.

II. PROVIDING TOKEN ASSURANCE DATA

[0148] The token assurance module 322 in the token processing server computer 202B can comprise code for implementing a method for generating a token assurance level or code associated with the token assurance level. The method may include receiving a token request from a token requester. The method may also include performing at least one authentication process associated with the token request, and in response to the performance of the at least one authentication process, generating, by the server computer, a token assurance code.

[0149] Any suitable authentication process or combination of authentication processes may be performed. The authentication may relate to the authentication of a payment device and/or the authentication of the consumer that will use the token. Examples of authentication processes that may be performed alone, or in combination, may include a verification value check such as a CVV or CVV2 check, an AVS (address verification service) check, a PAN and/or expiration date check (performed with a zero dollar or no dollar authorization request and response to an issuer, or performed by a payment processing network on behalf of an issuer), user password authentication checks (e.g., using a 3DS or 3D Secure type infrastructure), and one time password

(OTP) password verification. Other types of authentication processes that can be performed include device verification processes. For example, when requesting a payment token, a mobile phone may provide device characteristics such as a secure element identifier, a SIM card number, a phone number, an IMEI (International Mobile Station Equipment Identity) number, an MSISDN number, etc. Consumer information such as a birthday, home address, schools attended, etc. may also be used to authenticate the person using the token and the legitimacy of the token. Other examples of verification information can be stored in the card registration module 310 in FIG. 3 and are described above.

[0150] The token may then be transmitted to the token requester. The token assurance code may be stored in the token registry database 202A along with the token, for later retrieval and use. For example, the token assurance code may be passed, directly or indirectly, to a token requestor, an acquirer, a payment processing network, or an issuer during a payment process.

[0151] FIGs. 4A-4B illustrate exemplary methods for token requests authentication methods to determine token assurance level in one embodiment of the invention.

[0152] The token assurance level may be performed by the network token system 202 to authenticate the consumer, card credentials or the token at the time of the token request or afterwards. Referring back to FIG. 3, the token assurance level may be determined by the token assurance module 322. The token assurance level may be used for additional risk assessment by the payment processing network computer 160 or the issuer computer 170. For example, an assurance level code may be passed in the authorization request message to inform the level of assurance for that token in the transaction.

[0153] In step 402, the token requestor 204 may send a token request 402 to the token registry database 202A. The token request 402 may include a PAN, an expiration date, a CVV2, a full address of the consumer 110, a postal code and a token requestor

identifier. For example, the token request 402 may be a request for a token from the consumer device 120 (e.g., a wallet application) to initiate a transaction.

[0154] In step 404, the network token system 202 may provide a token response including a token assurance level, a token number and a token expiration date based on one or more authentication methods such as, but not limited to, a CVV2 check, an AVS check, an authentication process using a zero dollar authorization, an authentication process performed by a payment processing network (OBO) on behalf of an issuer, an authentication process using a 3DS (3D Secure) extension issuer ACS (access control server) or a 3DS (3D Secure) extension issuer OTP (one time password) process, as described below. It can be appreciated that the network token system 202 may provide the token response including the token assurance level after authenticating the cardholder using the one or more authentication methods. Each of the authentication methods are described in further detail below in transaction flows 1-6.

[0155] Transaction flow 1 illustrates a CVV2 check authentication method. In step 1A, when the token requestor 204 sends the token request 402, the token requestor 204 may also send the PAN associated with the payment account, the expiration date and a CVV2 value to the token vault 202A which may in turn send them to the payment processing network computer 160 for a CVV2 check. This information may have been provided by the user to the token requestor 204 prior to the token request 402. For example, the CVV2 value may be a security code associated with a payment card (e.g., three digit code printed on the card).

[0156] In step 1B, the payment processing network computer 160 may perform the CVV2 check and send a response message to the token registry 202A to approve or decline authorization of the user. For example, the payment processing network computer 160 may compare the CVV2 value provided by the consumer 120 with the CVV2 value on record (e.g., stored in the database of the payment processing network computer 160). If the CVV2 value matches what is stored in the database, the payment processing network computer 160 may authorize the user. When the token processing server computer 202B generates the token, the token processing server computer 202B

may realize that the user has been authenticated using a CVV2 check by the payment processing network computer 160 and may determine a token assurance level accordingly.

[0157] Transaction flow 2 illustrates an AVS check authentication method. In step 2A, when the token requestor 204 sends the token request 402, the requestor 204 may also send the PAN, expiration date, full address and the postal code associated with the cardholder to the token vault 202A which may in turn send them to the payment processing network computer 160. This information may have been provided by the cardholder (e.g., user) to the token requestor 204 prior to the token request 402. The AVS check enables elements of the billing address and the postal code provided by the consumer 110 to be compared against the issuer's records.

[0158] In step 2B, the payment processing network computer 160 may forward the PAN, expiration date, full address and the postal code to the issuer computer 170 for the AVS check.

[0159] In step 2C, the issuer computer 170 may perform the AVS check and may send a response message to the payment processing network computer 160 to approve or decline authorization of the user, for example, by comparing the billing address and the postal code provided by the consumer 110 with the data on record. For example, if the billing address and postal code provided match the data on record, the issuer computer 170 may authorize the user (e.g., cardholder or consumer).

[0160] In step 2D, the payment processing network computer 160 may forward the response message to the token registry 202A. When the token processing server computer 202B generates the token, the token processing server computer 202B may realize that the user has been authenticated using an AVS check by the payment processing network computer 160 and may determine a token assurance level accordingly.

[0161] Transaction flow 3 illustrates a zero dollar authorization authentication method. In step 3A, when the token requestor 204 sends the token request 402, the token requestor 204 may also send the PAN and the expiration date to the payment

processing network computer 160 in a zero dollar or no dollar authorization request message to the payment processing network 160. This information may have been provided by the user to the token requestor 204 prior to the token request 402.

[0162] In step 3B, the payment processing network computer 160 may forward the PAN, expiration date and the card-on-file indicator to the issuer computer 170 in the zero or no dollar authorization request message.

[0163] In step 3C, the issuer computer 170 may evaluate the PAN and expiration date to determine if they are authentic or fraudulent, and may send a response message to the payment processing network computer 160 to authenticate the user. For example, the issuer computer 170 may perform verification of the payment account number, personal identifier, address verification, and a card verification value (CVV, CVV2, or other variants, etc.) as part of the zero-dollar authorization request.

[0164] In step 3D, the payment processing network computer 160 may forward the response message to the token registry 202A. When the token processing server computer 202B generates the token, the token processing server computer 202B may realize that the user has been authenticated using an zero dollar authorization by the payment processing network computer 160 and may determine a token assurance level accordingly.

[0165] Transaction flow 4 illustrates a payment processing network OBO authentication method. In step 4A, when the token requestor 204 sends the token request 402, the token requestor 204 may also send the PAN and the expiration date to the token processing server computer 202B to perform the payment processing network authorization OBO. This information may have been provided by the user to the token requestor 204 prior to the token request 402.

[0166] In step 4B, the token processing server computer 202B may validate the PAN and the expiration date on-behalf-of (OBO) the issuer and send a response message to the token registry 202A to approve or decline authorization of the user accordingly. For example, if the PAN and expiration date can be verified on-behalf-of the issuer, the token processing server computer 202B may authorize the user. When

the token processing server computer 202B generates the token, the token processing server computer 202B may realize that the user has been authenticated using a payment processing network OBO check by the token processing server computer 202B and may determine a token assurance level accordingly.

[0167] Transaction flow 5 illustrates a 3D Secure extension issuer ACS authentication method. In step 5A, when the token requestor 204 sends the token request 402, the token requestor 204 may also send the PAN and the expiration date associated with the payment account directly to the issuer computer 170 for a 3DS extension issuer ACS check. This information may have been provided by the user to the token requestor 204 prior to the token request 402.

[0168] In step 5B, the issuer computer 170 may perform the ACS check and send a response message to the token registry database 202A to approve or decline authorization of the user. For example, the issuer computer 170 may query an appropriate ACS to authenticate the data with the data provided by the consumer 110 at the time of enrollment. The ACS could send a message to the consumer device 120 through a direct channel and may request that the consumer provide a PIN or other passcode to authenticate himself. If the user can be authenticated using the ACS, the issuer computer 170 may provide this information to the token processing server computer 202B. When the token processing server computer 202B generates the token, the token processing server computer 202B may realize that the user has been authenticated using a 3D Secure extension issuer ACS check by the payment processing network computer 160 and may determine a token assurance level accordingly.

[0169] Transaction flow 6 illustrates a 3D Secure extension issuer OTP authentication method. In step 6A, when the token requestor 204 sends the token request 402, the token requestor 204 may also send the PAN, expiration date and a one-time password (OTP) to the issuer computer 170 for a 3DS (3D Secure) extension issuer OTP (one time password) check. This information, with the exception of the

OTP, may have been provided by the user to the token requestor 204 prior to the token request 402.

[0170] In step 6B, the issuer computer 170 may provide the generated OTP (one time password) to the consumer device 120.

[0171] In step 6C, the consumer device 120 may provide the OTP (one time password) to the token requestor 204. For example, the token requestor 204 may be a mobile or a wallet application. The cardholder may have entered the OTP into the mobile or wallet application running on the consumer device 120.

[0172] In step 6D, the token requestor 204 may provide the OTP (one time password) to the token registry database 202A for validation of the OTP.

[0173] In step 6E, the token registry database 202A may verify the OTP and send a message to notify the issuer computer 170 to approve or decline the authentication of the user. For example, if the OTP received matches the generated OTP, the issuer computer 170 may authenticate the user. When the token processing server computer 202B generates the token, the token processing server computer 202B may realize that the user has been authenticated using a 3D Secure extension issuer OTP check by the payment processing network computer 160 and may determine a token assurance level accordingly.

[0174] It can be appreciated that transaction flows 1-6 described above may occur in between steps 402 and steps 404, or even before step 402. The token assurance levels described above may be represented in the form of a token assurance level field code that may be part of an authorization request message or an authorization response message.

[0175] A "token assurance code" may be any suitable value that represents a level of assurance that a particular token is authentic and/or can be trusted. In some embodiments, the token assurance code could include a score that is generated based upon factors such as the number or type of authentication processes performed, the payment channel, the authenticating entity, etc. For example, on a scale of 1-10, with

10 being the most trustworthy, a token assurance code of "8" may be assigned for a token that was issued after multiple authentication checks were performed on the user of the token and the payment device associated with the real PAN that is tied to the token. Alternatively, a token assurance code of "2" may be assigned to a token that was issued without any authentication processing performed prior to token issuance. In other embodiments, the token assurance code may represent original information about the authentication processes were performed, the payment channel, the authenticating entity, etc., without attempting to quantify the level of trust associated with such factors. For example, the token assurance code could simply be the number "2" to indicate that the token was issued after a CVV2 check was performed, and a "7" where a one time password authentication check was performed. The numbers "2" and "7" would simply be labels for the authentication processes performed, and would not necessarily indicate a specific level of trust. Other examples of factors that can be used in determining a token assurance level or code are provided below.

[0176] In some specific embodiments, the token assurance level code can indicate how the cardholder, card credential, and the token have been authenticated by the payment network. For example, the token assurance level code can indicate which of the above authentication methods were used to authenticate the cardholder when the token was requested and ultimately generated. These authentication methods include, but is not limited to, a CVV2 check, an AVS check, a zero dollar authorization, a payment processing network OBO, a 3DS extension issuer ACS, and a 3DS extension issuer OTP. During the course of a normal payment transaction, the token assurance level code can be used by the issuer 170 for additional risk assessment and to obtain a certain level of confidence that the user using the token is in fact the genuine cardholder.

[0177] In some specific embodiments, the token assurance level code may be a 2-digit number that indicates the token assurance level. For example, the token assurance level code may range from 00-99, with 00 being the lowest token assurance level and 99 being the highest token assurance level. It can be appreciated that any other indication scheme can be used for the token assurance level code.

[0178] The use of a token assurance level code to communicate risk within the payment network can have many advantages. First, the use of the token assurance level code can increase security within the payment network, particularly for payment transactions including the use of a token. Since the issuer 170 (and potentially other entities within the payment network) may be able to reference the token assurance level code in order to obtain a certain level of confidence that the token was legitimately generated and that it is being used by the genuine cardholder, the chances of approving a fraudulent transaction can be greatly reduced. Second, the use of a token assurance level code will increase efficiency of the payment system during a transaction since authentication processing for the token is not required. If an authorization request message is received by the issuer 170 that includes token assurance level code that indicates a relatively high token assurance level, the issuer 170 may simply authorize the transaction without the need for carrying out further authentication of the user and/or token. Further, as noted above, since a token is an obfuscated PAN, it is very difficult to perform the types of authentication processing that would normally be used when real PANs are used to conduct transactions. It can be appreciated that the use of the token assurance level code to communicate risk can provide many other advantageous described throughout this description.

[0179] Further advantages of using the token assurance level code to communicate risk within the payment network can be further illustrated in the examples described below.

[0180] FIG. 5 illustrates an exemplary transaction flow for near-field communication (NFC) at the point-of-sale (POS) according to some embodiments of the invention.

[0181] An authorization process 1102 for a transaction conducted at the POS using NFC may include steps 502A-502G.

[0182] The authorization process 502 may begin when a user wishes to conduct a transaction with a merchant. In step 502A, the NFC terminal at the merchant computer 140 may capture data from the user's consumer device 120 when the consumer device

120 is tapped or waved at the NFC terminal. For example, referring back to FIG. 1, the NFC terminal may be part of the access device 130 that may be communicatively coupled to the merchant computer 140. In one embodiment of the invention, in an off-line process, an issuer may have registered as a token requestor with the token vault and may have provisioned a token in a wallet application of the consumer device 120 (e.g., an NFC enabled cell phone). The consumer 110 may use the consumer device 120 to make a payment. The merchant computer 140 may capture a token, a token expiration date, a chip cryptogram and a POS entry mode from the consumer device 120. In one embodiment, a token requestor identifier may be hidden in the chip cryptogram data. The captured token may have been generated prior to the current transaction using any of the methods described in the description above.

[0183] In step 502B, the merchant computer 502B may generate an authorization request message with the captured data and provide it to the acquirer computer 150. The authorization request message may include additional fields such as transaction data, merchant identifier and any other relevant data. This data may include the token, token expiration date, chip cryptogram, and POS entry mode.

[0184] More specifically, in some embodiments, the authorization request message may include the following data fields: an amount data field; a primary account number data field (which holds the token); an expiration date field; a token presentment mode data field; a token requestor ID data field; a merchant data data fields such as a card acceptor ID data field, a merchant descriptor data field (merchant name), an MCC or merchant category code) data field, a merchant city data field, a merchant state data field, and a merchant postal code data field; a verification value data field (e.g., a dCVV data field); an issuer discretionary data data field, and a token assurance level code data field. A corresponding authorization response message may include some or all of these data fields.

[0185] In step 502C, the authorization request message may be conveyed to the payment processing network computer 160 by the acquirer computer 150. The

authorization request message may include the token, token expiration date, chip cryptogram, and POS entry mode.

[0186] In step 502D, the payment processing network computer 160 may decrypt the portions of the CHIP data containing the token requestor identifier and send the chip data, the token, the token expiration date, the token requestor identifier, a token assurance level, a PAN and a PAN expiration date to the issuer computer 170. For example, the payment processing network computer 160 may exchange the token for the PAN from the token vault and modify the authorization request message to include the PAN in place of the token before providing to the issuer computer 170. The modified authorization request message may also include the token requestor identifier and the token assurance level. Before sending the modified authorization request message to the issuer computer 170, the payment processing network computer 160 may validate that the token is being properly used in the correct domain. In some embodiments, the validation may be bypassed if the token assurance level is above a threshold assurance level.

[0187] In 502E, the issuer computer 170 may make an approval decision after receiving the modified authorization request message and send an authorization response message to the payment processing network 160. The approval decision may at least be based on the token assurance level code in the authorization request message. The token assurance level may indicate to the issuer computer 570 how the cardholder, card credential, and token have been authenticated by the token requestor. The token assurance level may be based on a number of factors.

[0188] One factor may include the assurance indicator which indicates which entity in the payment system authenticated the user or the account for the token generation. For example, the user may have been authenticated for the token generation by the token requestor, the payment processing network computer 560, the issuer 570, an ACS, or other entity. It can be appreciated that authentication by certain entities may affect the token assurance level more or less than authentication by other entities. For example, if the authentication was performed by the issuer computer 570,

then the token assurance level code may indicate a higher token assurance level than if the authorization was performed by the token requestor itself.

[0189] Another factor may include the date the date that the token was generated. Tokens generated closer to the date of the current transaction may have higher token assurance levels than those generated farther apart from the date of the current transaction. It can be appreciated that the token vault and/or token processor may keep a real-time record of the token assurance level associated with the token. The token assurance level may be updated at any time for a number of reasons pertaining to a number of variables, one of which may include how long ago the token was generated.

[0190] Another factor may include the wallet / device identification. The wallet / device identification may indicate which digital wallet and/or which device the token was generated for. Tokens generated for digital wallets and/or devices known to be more secure may have higher token assurance levels.

[0191] Another factor may include the number of successful (e.g., non-fraudulent) transactions that have been completed using the particular token. A greater number of successful transactions completed using the token may result in a higher token assurance level for the token. In some embodiments, the token vault and/or token processor may increase the token assurance level for the token upon each successful transaction, or vice versa.

[0192] The token assurance level as indicated by the token assurance level code may be determined based on a combination of any of the factors described above. The combination of factors may result in a determination of the overall token assurance level. The token assurance level may be updated at any time.

[0193] The approval decision may be made by the issuer based on the token assurance level. If the token assurance level is relatively low and below a threshold the issuer has set for approving a transaction, the transaction may be denied. If the token assurance level is relatively high and above a threshold the issuer has set for approving a transaction, the transaction may be approved. In some embodiments, the issuer may

base its approval/denial decision on the token assurance level combined with various other factors. For example, even if a token assurance level is low, if the token was received by the issuer computer 570 via a secure domain, the issuer computer 570 may still approve the transaction. In some embodiments, if the token assurance level is low, the issuer computer 570 may carry out further authentication procedures in order to attempt to authenticate the user and the token for the transaction, instead of simply denying the transaction.

[0194] In some embodiments, the token assurance information received in the authorization request message may also be used by the payment processing network computer 160 to generate a refined fraud score. Transaction fraud scores can be generated based on transaction characteristics such as the merchant that is conducting the transaction, the time of day, the date, the transaction velocity, the Internet address of the computer used to conduct the transaction, etc. Such information is used to create transaction fraud scores and the token assurance information can be used to create more refined and more accurate fraud scores that may be passed to the issuer computer 170 to help the issuer decide whether or not to authorize the transaction.

[0195] In some embodiments, the newly added fields (e.g., token assurance level) may be required to be “retained and returned” in the transaction.

[0196] In 502F, the payment processing network 160, upon receiving the response, may swap the PAN for the token, optionally populate the last four digits of the PAN in the authorization response message, and return the token assurance level in the modified authorization response message to the acquirer computer 150. The modified authorization response message may also include a PAN product identifier.

[0197] In 502G, the acquirer computer 150 may forward the authorization response message to the merchant computer 540.

[0198] A clearing and exception process 504 may include steps 504A-504D as described below. For example, the clearing and exception process may be performed by a clearing module to reconcile the transaction order.

[0199] In step 504A, the acquirer computer 150 may submit a clearing draft message with the token in the PAN field, along with CHIP data to the payment processing network 160. The clearing draft message may also include a token assurance level.

[0200] In step 504B, the clearing process at the payment processing network 160 may recognize the token and replace the token with the real PAN (e.g., from the token vault) in the clearing draft to the issuer computer 170. The clearing process may place the token in a new field in the clearing draft message to the issuer computer 170, also populating the token assurance level.

[0201] In step 504C, should a chargeback occur, the issuer computer 170 may retain and return the token as well as the PAN to the payment processing network 160. In some embodiments, liability for the chargeback may fall on various entities in the payment network based upon the token assurance level. For example, if an entity proceeded with the transaction despite a low token assurance level, the liability for the chargeback may fall on that entity.

[0202] In step 504D, the clearing process may move the token to the PAN field and drop the real PAN from the clearing draft message to the acquirer computer 150.

[0203] FIG. 6 illustrates shows an exemplary flow diagram for card-on-file/e-commerce transaction according to one embodiment of the invention.

[0204] In step 602A, the consumer 110 may make a purchase using the consumer device 120. As an off-line process, prior to the transaction, the merchant (e.g., online merchant) may have registered for a token requestor identifier. Also as an off line process, the merchant may batch request all of their PANs, getting a corresponding token. In this implementation, the token may be related to a specific merchant.

[0205] In step 602B, the merchant computer 140 may initiate an authorization request message to the acquirer computer 150. When the authorization is initiated, the merchant/acquirer may provide a token in place of the PAN and a token expiration date.

[0206] In step 602C, the acquirer computer 150 may forward the authorization request message to the payment processing network computer 160.

[0207] In step 602D, the payment processing network computer 160 may recognize that the token is from a token enabled merchant and replace the token with the real PAN (e.g., from the token vault) and send the token in a new field, the token requestor identifier, and token assurance level and the PAN to the issuer computer 170 in a modified authorization request message. The token requestor identifier and token assurance level may be optional for issuers.

[0208] In 602E, the issuer computer 170 may make an approval decision and send an authorization response message to the payment processing network 160. The newly added fields (e.g., token assurance level) may be required to be “retained and returned” in the transaction.

[0209] In 602F, the payment processing network 160, upon receiving the response, may swap the PAN for the token, optionally populate the last four digits of the PAN in the authorization response message, and return the token assurance level in the modified authorization response message to the acquirer computer 150. The modified authorization response message may also include a PAN product identifier.

[0210] In 602G, the acquirer computer 150 may forward the authorization response message to the merchant computer 602G.

[0211] A clearing and exception process 604 may include steps 604A-604D as described below. For example, as discussed with reference to FIG. 5, the clearing and exception process may be performed by the clearing module 518 to reconcile the transaction order.

[0212] In step 604A, the acquirer computer 150 may submit a clearing draft message with the token in the PAN field, along with CHIP data to the payment processing network 160. The clearing draft message may also include a token assurance level.

[0213] In step 604B, the clearing process at the payment processing network 160 may recognize the token and replace the token with the real PAN (e.g., from the token vault) in the clearing draft message to the issuer computer 170. The clearing process may place the token in a new field in the clearing draft message to the issuer computer 170, also populating the token assurance level.

[0214] In step 604C, should a chargeback occur, the issuer computer 170 may retain and return the token as well as the PAN to the payment processing network 160.

[0215] In step 604D, the clearing process may move the token to the PAN field and drop the real PAN from the clearing draft message to the acquirer computer 150.

[0216] It can be appreciated that FIG. 6 is similar to FIG. 5 except that FIG. 6 illustrates a card-on-file transaction instead of an NFC-based transaction. The processes and methods described with respect to token assurance levels apply in their entirety to FIG. 6. It can be appreciated that some of the data passed in authorization request messages differs to what is shown in FIG. 5 because a card-on-file transaction may be associated with different data than an NFC-based transaction.

[0217] FIG. 7 is a flowchart of an exemplary method 700 for transmitting a token assurance level code to an issuer or other entity, in accordance with some embodiments of the invention. In block 702, an authorization request message including a payment token is received. The payment token may be associated with a real account identifier. In some embodiments, the authorization request message is received by a server computer from a merchant computer. In some embodiments, before receiving the authorization request message, the payment token may be generated and provided to the server computer by an issuer.

[0218] In block 704, after receiving the authorization request message, the real account identifier associated with the payment token is determined.

[0219] In block 706, after determining the real account identifier associated with the payment token, a modified authorization request message including the real account identifier is generated. The modified authorization request message may include the

real account identifier and a token assurance level code indicative of a level of risk associated with the payment token. The level of risk may indicate whether the payment token was requested by a genuine account holder of the underlying payment account associated with the real account identifier. The token assurance level code may also indicate an authentication method associated with generation of the payment token. The authentication method can include, but is not limited to, no authentication, network authentication, or issuer authentication. Additionally, the token assurance level code may be based at least in part on a transaction history associated with the real account identifier. In some embodiments, the token assurance level code is generated at the time the payment token is generated.

[0220] In block 708, after generating the modified authorization request message, the modified authorization request message is transmitted to an issuer for approval. The issuer approval may be based at least in part on the token assurance level code.

[0221] The network token system as discussed with different embodiments provides a platform that can be leveraged by external entities (e.g., third party wallets, e-commerce merchants, payment enablers / payment service providers, etc.) or internal payment processing network systems that have the need to use the token to facilitate payment transactions. In embodiments of the invention, a token can support interoperability and can be accepted, processed and routed by the entities within the payment system. Embodiments of the invention can help card issuers and merchants improve card security or enable new payment experiences through tokenization.

[0222] The various participants and elements described herein with reference to FIGs. 1 and 2 may operate one or more computer apparatuses to facilitate the functions described herein. Any of the elements in FIGs. 1 and 2, including any servers or databases, may use any suitable number of subsystems to facilitate the functions described herein.

[0223] Examples of such subsystems or components are shown in FIG. 8. The subsystems shown in FIG. 8 are interconnected via a system bus 810. Additional subsystems such as a printer 830, keyboard 818, fixed disk 820 (or other memory

comprising computer readable media), monitor 812, which is coupled to display adapter 814, and others are shown. Peripherals and input/output (I/O) devices, which couple to I/O controller 824 (which can be a processor or other suitable controller), can be connected to the computer system by any number of means known in the art, such as serial port 816. For example, serial port 816 or external interface 822 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 allows the central processor 828 to communicate with each subsystem and to control the execution of instructions from system memory 826 or the fixed disk 820, as well as the exchange of information between subsystems. The system memory 826 and/or the fixed disk 820 may embody a computer readable medium.

[0224] 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.

[0225] The above description is illustrative and is 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 above description, but instead should be determined with reference to the pending claims along with their full scope or equivalents.

[0226] 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.

[0227] A recitation of "a", "an" or "the" is intended to mean "one or more" unless specifically indicated to the contrary.

[0228] All patents, patent applications, publications, and descriptions mentioned above are herein incorporated by reference in their entirety for all purposes. None is admitted to be prior art.

WHAT IS CLAIMED IS:

- 1 1. A method, comprising:
2 receiving, by a server computer, a token request from a token requester;
3 performing, by the server computer, at least one authentication process
4 associated with the token request;
5 in response to the performance of the at least one authentication process,
6 generating, by the server computer, a token assurance code; and
7 transmitting, by the server computer, the token to the token requester.
- 1 2. The method of claim 1 further comprising storing the token
2 assurance code in a token registry database.
- 1 3. The method of claim 1 wherein the at least one authentication
2 process comprises an authentication process selected from the group consisting of a
3 CVV2 check, an AVS check, and a one time password (OTP) verification check.
- 1 4. The method of claim 1, wherein the token request comprises an
2 account identifier associated with a credit or debit card.
- 1 5. The method of claim 1 further comprising:
2 retrieving the token assurance code from the token registry database; and
3 providing the token assurance code to a payment processing network
4 after the payment processing network receives an authorization request message for a
5 transaction conducted with the token.
- 1 6. A server computer comprising a processor, and a computer
2 readable medium coupled to the processor, the computer readable medium comprising
3 code, executable by the processor, for implementing a method comprising:
4 receiving a token request from a token requester;
5 performing at least one authentication process associated with the token
6 request;

7 in response to the performance of the at least one authentication process,
8 generating a token assurance code; and
9 transmitting the token to the token requester.

1 7. The server computer of claim 6, wherein the method further
2 comprises:
3 storing the token assurance code in a token registry database.

1 8. The server computer of claim 6, wherein the at least one
2 authentication process comprises an authentication process selected from the group
3 consisting of a CVV2 check, an AVS check, and a one time password (OTP) verification
4 check.

1 9. The server computer of claim 6, wherein the token request
2 comprises an account identifier associated with a credit or debit card.

1 10. The server computer of claim 6, further comprising:
2 retrieving the token assurance code from the token registry database; and
3 providing the token assurance code to a payment processing network
4 after the payment processing network receives an authorization request message for a
5 transaction conducted with the token.

1 11. A method, comprising:
2 receiving, by a server computer, an authorization request message
3 comprising a payment token, wherein the payment token is associated with a real
4 account identifier;
5 determining, by the server computer, the real account identifier associated
6 with the payment token;
7 generating, by the server computer, a modified authorization request
8 message comprising the real account identifier, wherein the modified authorization
9 request comprises a token assurance level code indicative of a level of confidence
10 associated with the payment token; and

11 transmitting, by the server computer, the modified authorization request
12 message to an issuer for approval.

1 12. The method of claim 11, wherein the level of confidence associated
2 with the payment token comprises a level of confidence that the payment token was
3 requested by an account holder of an underlying payment account associated with the
4 real account identifier.

1 13. The method of claim 11, wherein the token assurance level code
2 indicates an authentication method associated with the payment token.

1 14. The method of claim 13, wherein the authentication method
2 comprises at least one of: no authentication, network authentication, or issuer
3 authentication.

1 15. The method of claim 11, wherein the token assurance level code is
2 based at least in part on a transaction history associated with the real account identifier.

1 16. A server computer comprising a processor and a computer
2 readable medium comprising code, executable by the processor, for implementing a
3 method comprising:

4 determining, by the server computer, the real account identifier associated
5 with the payment token;

6 generating, by the server computer, a modified authorization request
7 message comprising the real account identifier, wherein the modified authorization
8 request comprises a token assurance level code indicative of a level of confidence
9 associated with the payment token; and

10 transmitting, by the server computer, the modified authorization request
11 message to an issuer for approval.

1 17. The server computer of claim 16, wherein the issuer approval is
2 based at least in part on the token assurance level code.

1 18. The server computer of claim 16, wherein the level of confidence
2 associated with the payment token comprises a level of confidence that the payment
3 token was requested by an account holder of an underlying payment account
4 associated with the real account identifier.

1 19. The server computer of claim 16, wherein the token assurance
2 level code indicates an authentication method associated with the payment token.

1 20. The server computer of claim 19, wherein the authentication
2 method comprises at least one of: no authentication, network authentication, or issuer
3 authentication.

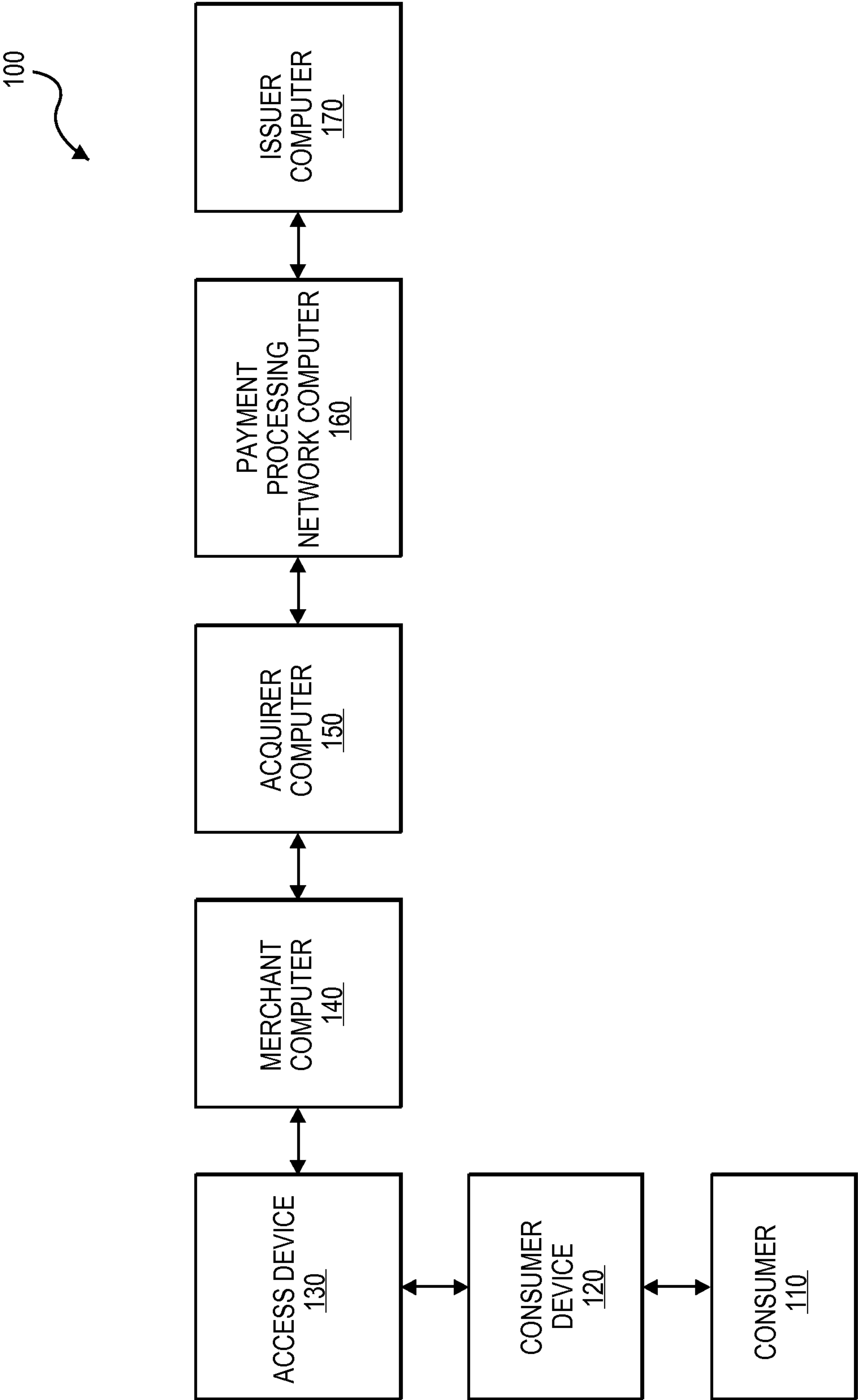


FIG. 1

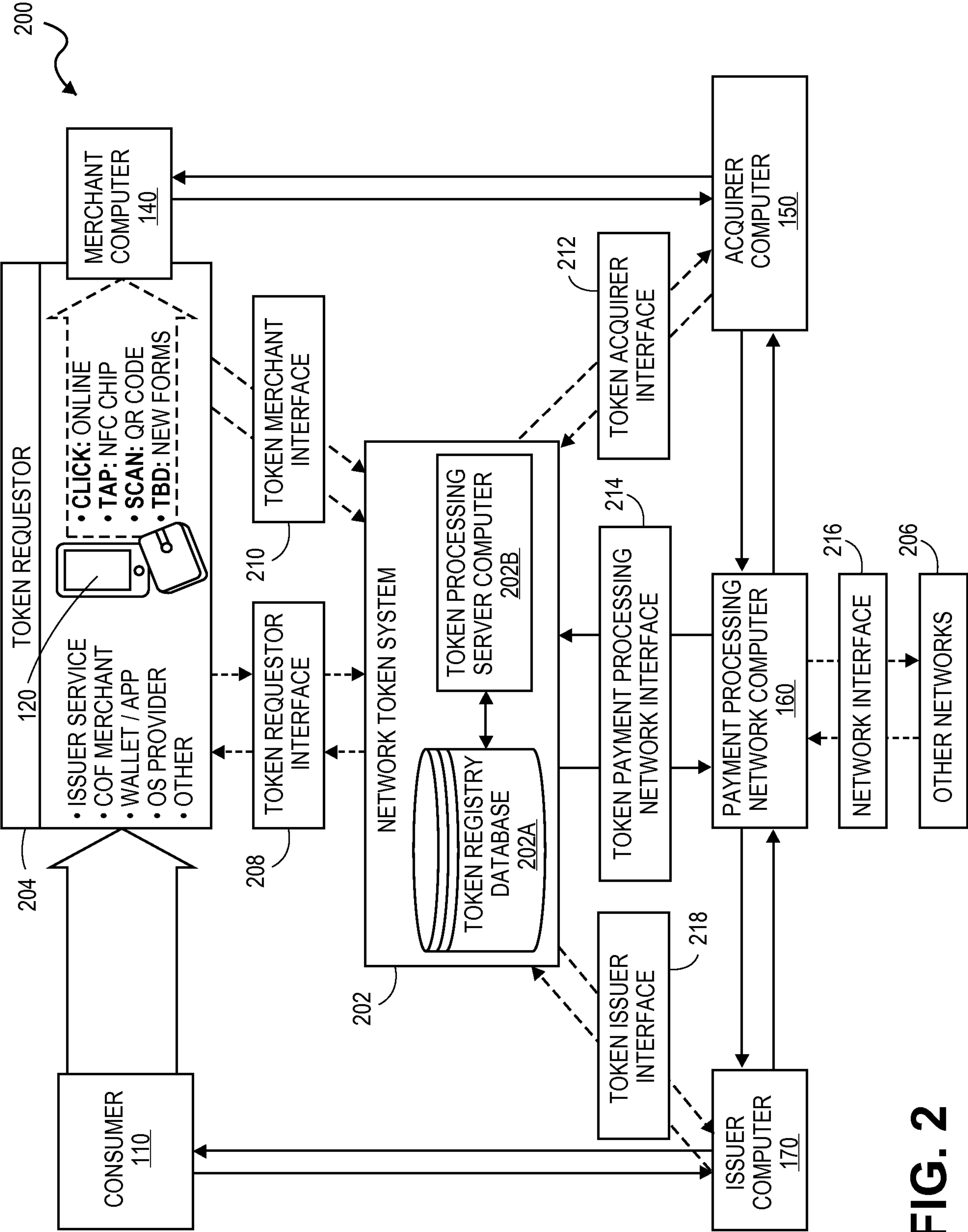
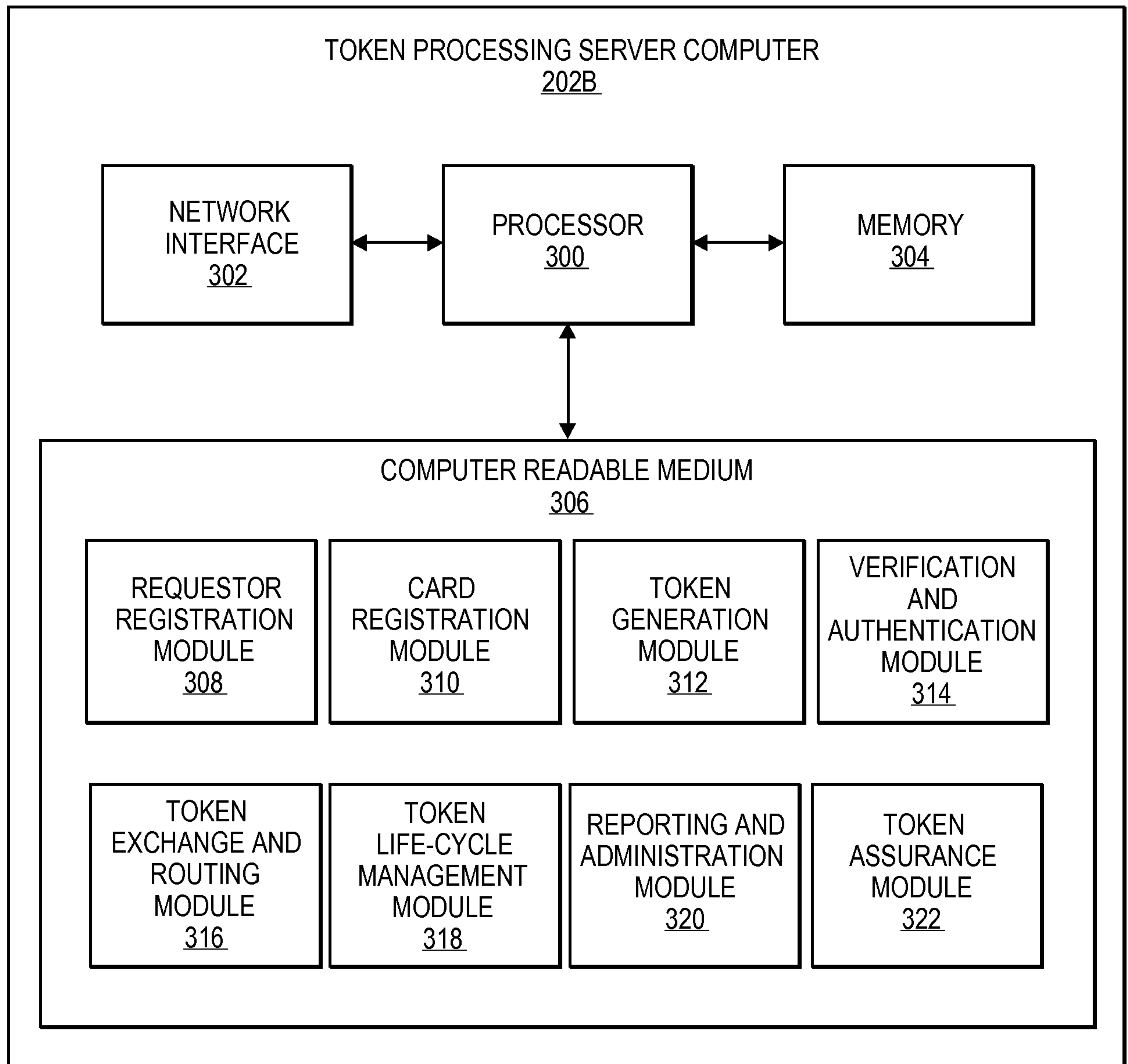


FIG. 2

3/9

**FIG. 3**

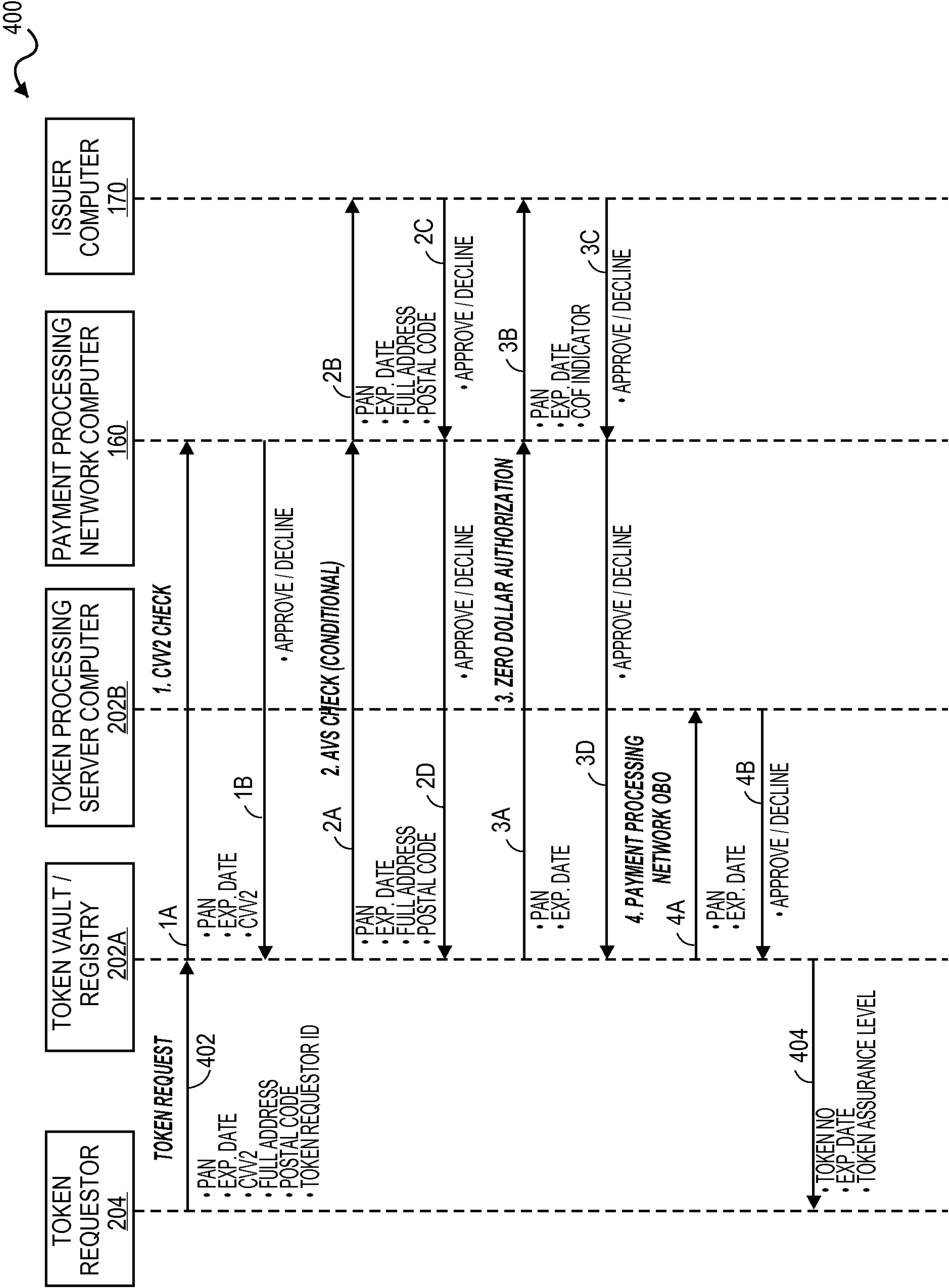


FIG. 4A

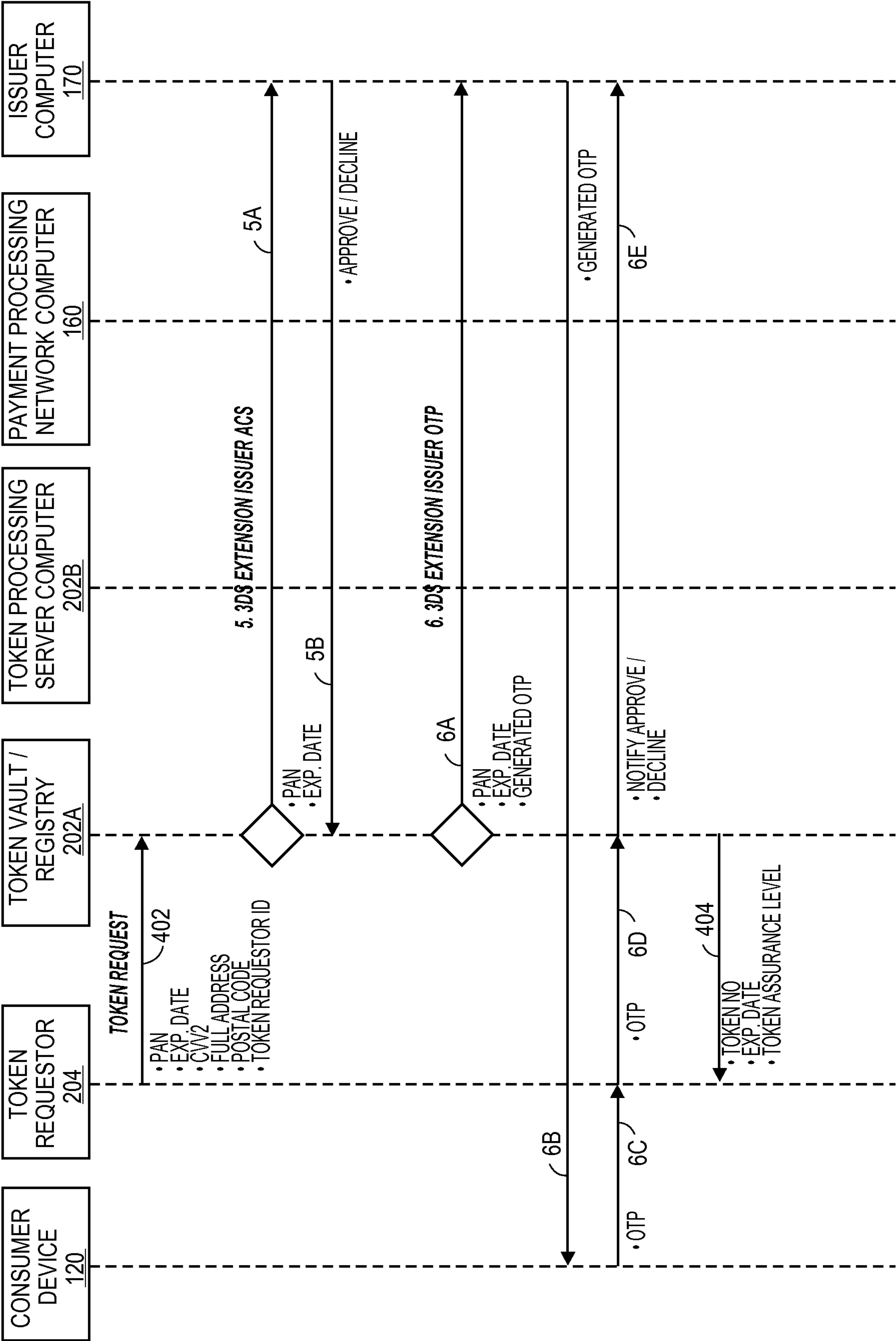


FIG. 4B

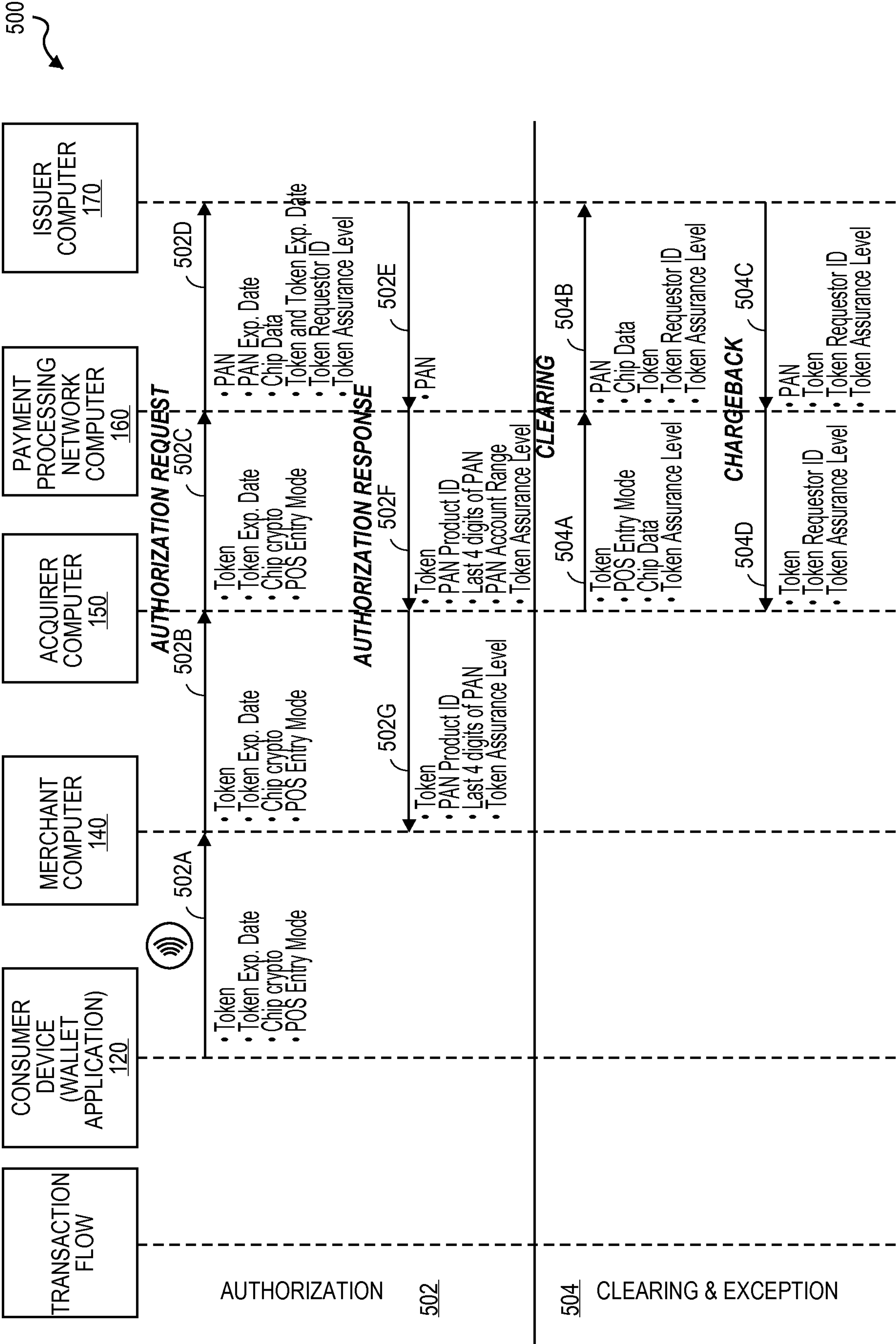


FIG. 5

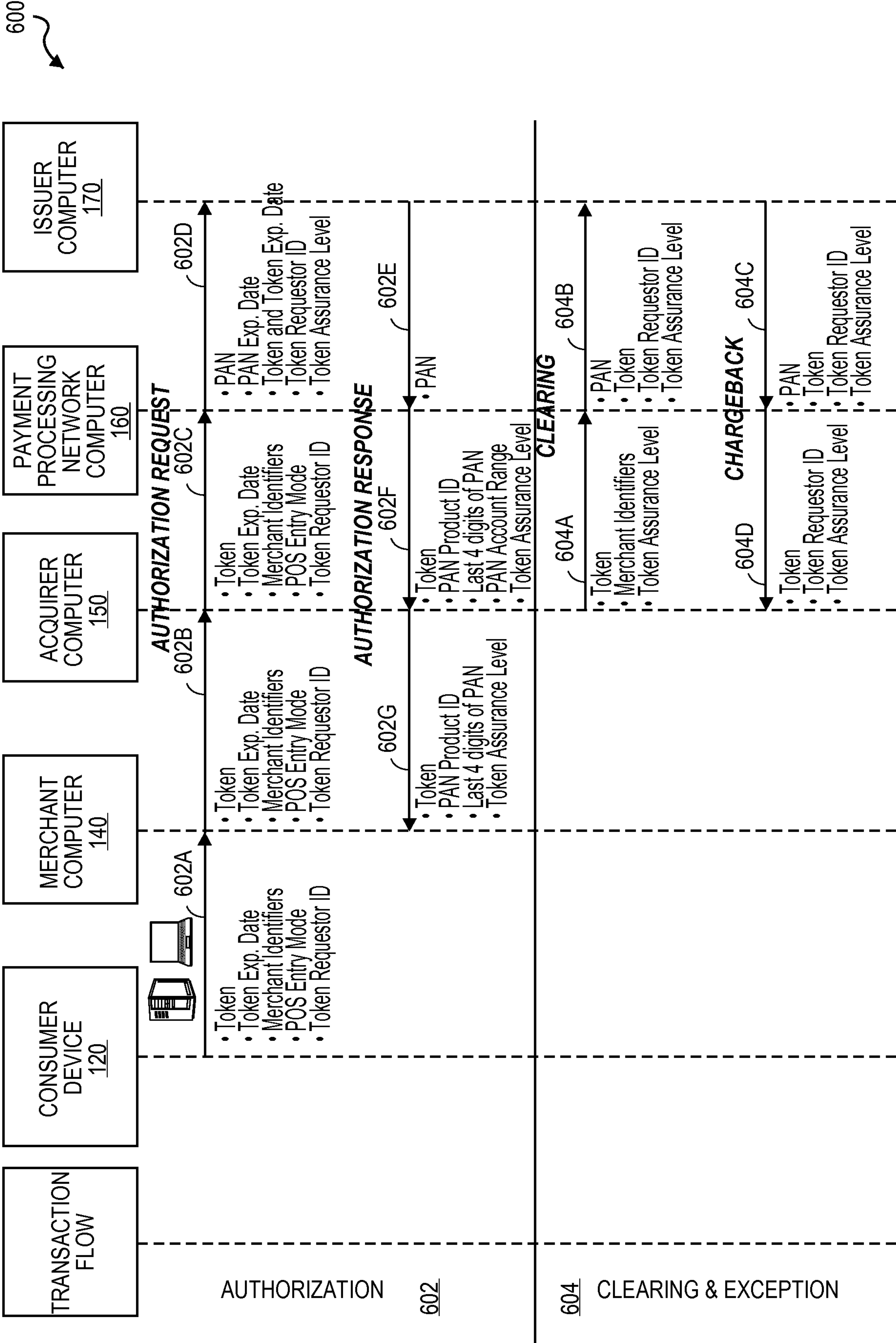
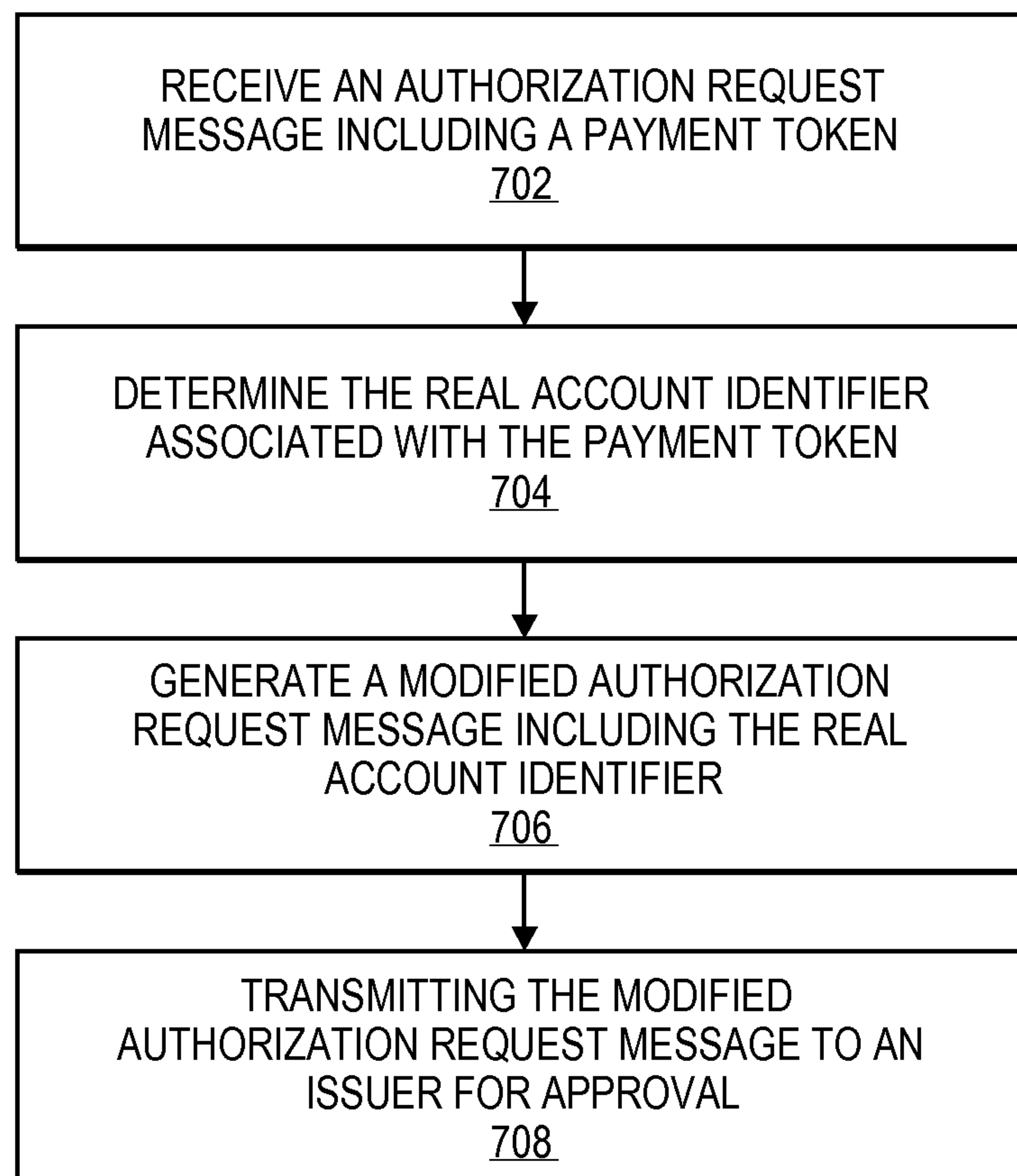


FIG. 6

8/9

**FIG. 7**

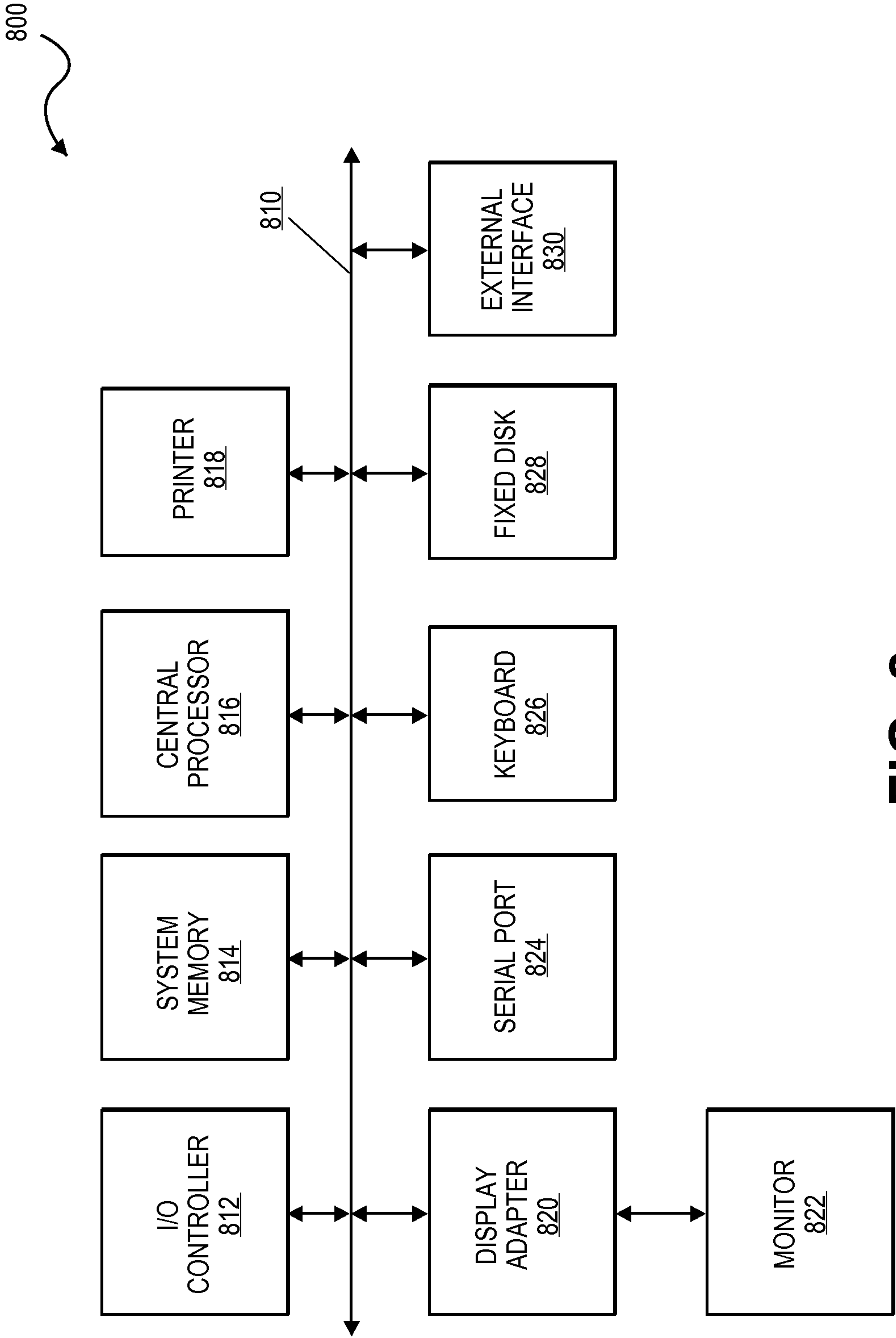


FIG. 8

