

INTERACTION ACCOUNT TOKENIZATION SYSTEM AND METHOD

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] None.

BACKGROUND

5 **[0002]** User to user interactions can occur when one user initiates an interaction with another user to transfer data, share a Wi-Fi connection, transfer an amount, etc. The users may or may not know one another. However, during the interaction, sensitive data such as an account name/number can be provided to the other user in order to complete the interaction. Each user's confidentiality is compromised with current user
10 to user interactions.

[0003] Furthermore, these types of user to user interactions can also risk the users' security by providing account names/numbers to the other user. A malicious user can attempt to fraudulently utilize received account names/numbers.

[0004] Interactions may also require either the receiver or the sender, or both, to
15 securely store the account names/numbers of other users. Each user needs to have increased security capabilities (e.g., hardware and software) to securely store this sensitive data. This presents not only security concerns, but also complexity concerns.

[0005] Embodiments of the disclosure address this problem and other problems individually and collectively.

20 SUMMARY

[0006] Embodiments are related to methods and systems for interaction account tokenization processing.

[0007] One embodiment is related to a method comprising: receiving, by a tokenization computer from a processing network computer, a tokenization request
25 message during an interaction between a first user device and a second user device,

wherein the tokenization request message comprises first user account data and second user account data; selecting, by the tokenization computer, a tokenization option of a plurality of tokenization options in a tokenization matrix based on the first user account data and the second user account data; determining, by the tokenization computer, alternate first user account data and alternate second user account data based on the tokenization option; generating, by the tokenization computer, a tokenization response message comprising the alternate first user account data and the alternate second user account data; and providing, by the tokenization computer, the tokenization response message to the processing network computer.

10 **[0008]** Another embodiment is related to a tokenization computer comprising: a processor; and a computer-readable medium coupled to the processor, the computer-readable medium comprising code executable by the processor for implementing a method comprising: receiving, by a tokenization computer from a processing network computer, a tokenization request message during an interaction between a first user device and a second user device, wherein the tokenization request message comprises first user account data and second user account data; selecting, by the tokenization computer, a tokenization option of a plurality of tokenization options in a tokenization matrix based on the first user account data and the second user account data; determining, by the tokenization computer, alternate first user account data and alternate second user account data based on the tokenization option; generating, by the tokenization computer, a tokenization response message comprising the alternate first user account data and the alternate second user account data; and providing, by the tokenization computer, the tokenization response message to the processing network computer.

25 **[0009]** Another embodiment is related to a method comprising: receiving, by an authorizing entity computer, an interaction request message from a first user device comprising an amount, first user account data, and second user account data; determining, by the authorizing entity computer, whether or not to authorize the interaction; if the interaction is authorized, determining, by the authorizing entity computer, a tokenization flag that indicates whether or not to tokenize the first user

30

account data; modifying, by the authorizing entity computer, the interaction request message to include the tokenization flag; and providing, by the authorizing entity computer, the interaction request message to a processing network computer, wherein the processing network computer provides a tokenization request message comprising
5 the first user account data, the second user account data, and the tokenization flag to a tokenization computer, wherein the tokenization computer selects a tokenization option of a plurality of tokenization options in a tokenization matrix based on the first user account data and the second user account data, determines alternate first user account data and alternate second user account data based on the tokenization option, and
10 generates a tokenization response message comprising the alternate first user account data and the alternate second user account data.

[0010] Further details regarding embodiments of the disclosure can be found in the Detailed Description and the Figures.

BRIEF DESCRIPTION OF THE DRAWINGS

15 **[0011]** FIG. 1 shows a block diagram of a tokenization system according to embodiments.

[0012] FIG. 2 shows a block diagram of components of a tokenization computer according to embodiments.

20 **[0013]** FIG. 3 shows a flow diagram of an account tokenization and interaction method according to embodiments.

[0014] FIG. 4 shows a tokenization matrix according to embodiments.

[0015] FIG. 5 shows a flow diagram of a token initiation and interaction method according to embodiments.

DETAILED DESCRIPTION

25 **[0016]** Prior to discussing embodiments of the disclosure, some terms can be described in further detail.

[0017] A “user” may include an individual. In some embodiments, a user may be associated with one or more personal accounts and/or mobile devices. The user may also be referred to as a cardholder, account holder, or consumer in some embodiments.

5 **[0018]** A “user device” may be a device that is operated by a user. Examples of user devices may include a mobile phone, a smart phone, a card, a personal digital assistant (PDA), a laptop computer, a desktop computer, a server computer, a vehicle
10 such as an automobile, a thin-client device, a tablet PC, etc. Additionally, user devices may be any type of wearable technology device, such as a watch, earpiece, glasses, etc. The user device may include one or more processors capable of processing user input. The user device may also include one or more input sensors for receiving user
15 input. As is known in the art, there are a variety of input sensors capable of detecting user input, such as accelerometers, cameras, microphones, etc. The user input obtained by the input sensors may be from a variety of data input types, including, but not limited to, audio data, visual data, or biometric data. The user device may comprise
any electronic device that may be operated by a user, which may also provide remote communication capabilities to a network. Examples of remote communication capabilities include using a mobile phone (wireless) network, wireless data network (e.g., 3G, 4G or similar networks), Wi-Fi, Wi-Max, or any other communication medium that may provide access to a network such as the Internet or a private network.

20 **[0019]** A “user identifier” can include any piece of data that can identify a user. A user identifier can comprise any suitable alphanumeric string of characters. In some embodiments, the user identifier may be derived from user identifying information. In some embodiments, a user identifier can include an account identifier associated with the user.

25 **[0020]** An “interaction” may include a reciprocal action or influence. An interaction can include a communication, contact, or exchange between parties, devices, and/or entities. Example interactions include a transaction between two parties and a data exchange between two devices. In some embodiments, an interaction can include a user requesting access to secure data, a secure webpage, a secure location,

and the like. In other embodiments, an interaction can include a payment transaction in which two devices can interact to facilitate a payment.

[0021] “User account data” can include one or more pieces of information regarding a record. User account data can include data that identifies and/or is associated with an account maintained for a user. For example, user account data can be a real account number or a token.

[0022] “Alternate user account data” can include one or more other pieces of information regarding a record. Alternate user account data can be user account data. In some embodiments, if user account data is a real account number, then the alternate user account data can be a token. As another example, if user account data is a token, then the alternate user account data can be a real account number. However, it is understood that the alternate user account data can be the same data as the user account data based on, for example, a tokenization flag in a tokenization matrix.

[0023] A “tokenization flag” can include a variable used to indicate a particular property (tokenization) of data. A tokenization flag can indicate whether or not user account data is to be tokenized during an interaction. In some embodiments, a tokenization flag can be a Boolean value that indicates “True” or “False.”

[0024] A “token” may be a substitute value for a credential. A token may be a string of numbers, letters, or any other suitable characters. Examples of tokens include payment tokens, access tokens, personal identification tokens, etc.

[0025] A “payment token” may include an identifier for a payment account that is a substitute for an account identifier, such as a primary account number (PAN). For example, a payment token may include a series of alphanumeric characters that may be used as a substitute for an original account identifier. For example, a token “4900 0000 0000 0001” may be used in place of a PAN “4147 0900 0000 1234.” In some embodiments, a payment token may be “format preserving” and may have a numeric format that conforms to the account identifiers used in existing transaction processing networks (e.g., ISO 8583 financial transaction message format). In some embodiments, a payment 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 payment token 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

5 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.

[0026] “Tokenization” is a process by which data is replaced with substitute data. For example, a payment account identifier (e.g., a primary account number (PAN)) may be tokenized by replacing the primary account identifier with a substitute number (e.g. a
10 token) that may be associated with the payment account identifier. Further, tokenization may be applied to any other information that may be replaced with a substitute value (i.e., token). Tokenization enhances transaction efficiency and security.

[0027] A “tokenization computer” can include a system that services tokens. In some embodiments, a tokenization computer can facilitate requesting, determining
15 (e.g., generating) and/or issuing tokens, as well as maintaining an established mapping of tokens to primary account numbers (PANs) in a repository (e.g. token vault). In some embodiments, the tokenization computer may establish a token assurance level for a given token to indicate the confidence level of the token to PAN binding. The tokenization computer may include or be in communication with a token vault where the
20 generated tokens are stored. The tokenization computer may support token processing of interactions (e.g., payment transactions) submitted using tokens by de-tokenizing the tokens to obtain the actual PANs. In some embodiments, a tokenization other computers such as a processing network computer. Various entities of a tokenization ecosystem may assume the roles of the tokenization computer operator. For example,
25 payment networks and issuers or their agents may become the tokenization computer operator by implementing the token services according to embodiments of the present invention.

[0028] A “token expiry date” may refer to the expiration date/time of the token. The token expiry date may be passed among the entities of the tokenization ecosystem
30 during transaction processing to ensure interoperability. The token expiration date may

be a numeric value (e.g. a 4-digit numeric value). In some embodiments, the token expiry date can be expressed as a time duration as measured from the time of issuance.

[0029] A “tokenization request message” may be an electronic message for requesting a token. A tokenization request message may include information usable for identifying an account such as a payment account or digital wallet, and/or information for generating a token such as a payment token. For example, a tokenization request message can comprise first user account data (e.g., a first user real account number, a first user token, etc.) and second user account data (e.g., a second user real account number, a second user token, etc.). As an additional example, a tokenization request message may include payment credentials, mobile device identification information (e.g. a phone number or MSISDN), a digital wallet identifier, information identifying a tokenization computer, a cryptogram, and/or any other suitable information. Information included in a tokenization request message can be encrypted (e.g., with an issuer-specific key).

[0030] A “tokenization response message” may be a message that responds to a token request. A tokenization response message may include an indication that a token request was approved or denied. For example, a tokenization response message can comprise alternate first user account data (e.g., a first user real account number, a first user token, etc.) and the alternate second user account data (e.g., a second user real account number, a second user token, etc.). A tokenization response message may also include a token, mobile device identification information (e.g. a phone number or MSISDN), a digital wallet identifier, information identifying a tokenization computer, a cryptogram, and/or any other suitable information. Information included in a tokenization response message can be encrypted (e.g., with an issuer-specific key).

[0031] A “tokenization matrix” can include an array of tokenization data. A tokenization matrix can include a plurality of rows and columns that include tokenization data. A row in a tokenization matrix can be a tokenization option. A tokenization matrix can be utilized to determine one or more processes to determine altered user account data from user account data. A tokenization matrix can include any suitable number of

columns relating to each tokenization option. A tokenization matrix can include columns relating to first user account data, a first tokenization flag, second user account data, a second tokenization flag, alternate first user account data (or a process to obtain alternate first user account data), and alternate second user account data (or a process to obtain alternate first user account data).

[0032] “Tokenization options” can include tokenization processes that may be chosen. A tokenization option can be a row in a tokenization matrix. A tokenization option can include one or more tokenization flags. For example, a tokenization option can include a first tokenization flag received from, and set by, a first authorizing entity computer and a second tokenization flag received from, and set by, a second authorizing entity computer. A tokenization computer can determine a particular tokenization option based on received first user account data and second user account data, and in some embodiments, the first tokenization flag and the second tokenization flag. Alternate user account data can be determined using the appropriate tokenization option in the tokenization matrix.

[0033] A “processing network computer” may include a server computer used for processing network data. In some embodiments, the processing network computer may be coupled to a database and may include any hardware, software, other logic, or combination of the preceding for servicing the requests from one or more client computers. The processing network computer may comprise one or more computational apparatuses and may use any of a variety of computing structures, arrangements, and compilations for servicing the requests from one or more client computers. In some embodiments, the processing network computer may operate multiple server computers. In such embodiments, each server computer may be configured to process transaction for a given region or handles transactions of a specific type based on transaction data.

[0034] The processing network computer may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. An exemplary processing network computer may include VisaNet™. Networks that include VisaNet™

are able to process credit card transactions, debit card transactions, and other types of commercial transactions. VisaNet™, in particular, includes an integrated payments system (Integrated Payments system) which processes authorization requests and a Base II system, which performs clearing and settlement services. The processing network computer may use any suitable wired or wireless network, including the Internet.

[0035] “Credentials” may comprise any evidence of authority, rights, or entitlement to privileges. For example, access credentials may comprise permissions to access certain tangible or intangible assets, such as a building or a file. Examples of credentials may include passwords, passcodes, or secret messages. In another example, payment credentials may include any suitable information associated with and/or identifying an account (e.g., a payment account and/or payment device associated with the account). Such information may be directly related to the account or may be derived from information related to the account. Examples of account information may include an “account identifier” such as a PAN (primary account number or “account number”), a token, a subtoken, a gift card number or code, a prepaid card number or code, a user name, an expiration date, a CVV (card verification value), a dCVV (dynamic card verification value), a CVV2 (card verification value 2), a CVC3 card verification value, etc. An example of a PAN is a 16-digit number, such as “4147 0900 0000 1234”. In some embodiments, credentials may be considered sensitive information.

[0036] A “cryptogram” may include a piece of obscured text such as encrypted text. A cryptogram may be formed by encrypting input data with an encryption key such as a symmetric encryption key. In some embodiments, a cryptogram is reversible so that the inputs that are used to form the cryptogram can be obtained using the same symmetric key to perform a decryption process. In some embodiments, if input data is encrypted using a private key of a public/private key pair, the cryptogram may also be a digital signature. A digital signature may be verified with a public key of the public/private key pair. In some embodiments, a cryptogram may include a dCVV (dynamic card verification value).

[0037] The term “verification” and its derivatives may refer to a process that utilizes information to determine whether an underlying subject is valid under a given set of circumstances. Verification may include any comparison of information to ensure some data or information is correct, valid, accurate, legitimate, and/or in good standing.

5 **[0038]** An “authorizing entity” may be an entity that authorizes a request. Examples of an authorizing entity may be an issuer, a governmental agency, a document repository, an access administrator, etc.

[0039] An “issuer” may typically refer to a business entity (e.g., a bank) that maintains an account for a user. An issuer may also issue payment credentials stored
10 on a user device, such as a cellular telephone, smart card, tablet, or laptop to the consumer.

[0040] A “processor” may include a device that processes something. In some embodiments, a processor can include any suitable data computation device or devices. A processor may comprise one or more microprocessors working together to
15 accomplish a desired function. The processor may include a CPU comprising 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
20 the like processor(s).

[0041] A “memory” may be any suitable device or devices that can store electronic data. A suitable memory may comprise a non-transitory computer readable medium that stores instructions that can be executed by a processor to implement a desired method. Examples of memories may comprise one or more memory chips, disk
25 drives, etc. Such memories may operate using any suitable electrical, optical, and/or magnetic mode of operation.

[0042] A “server computer” may include a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the

server computer may be a database server coupled to a Web server. The server computer may comprise one or more computational apparatuses and may use any of a variety of computing structures, arrangements, and compilations for servicing the requests from one or more client computers.

5 **[0043]** Embodiments of the disclosure allow for user to user interactions utilizing user account data that can include real account numbers and/or tokens. Various embodiments, allow for tokenization, without the need for authorizing entity computers (e.g., various financial institutions) to make any changes to existing interfaces, thus creating a frictionless experience. For this, a tokenization computer can connect to a
10 tokenization computer (e.g., via a processing network computer) and tokenize and/or detokenize originating user (e.g., first user) data and recipient user (e.g., second user) data based on a tokenization matrix. The tokenization computer can store a tokenization matrix comprising a plurality of tokenization options that can allow the tokenization computer to determine which account values to tokenize or tokens to
15 detokenize. Further, the tokenization matrix can include tokenization flags for the originator user and the receiver user that indicate whether or not to perform the tokenization and/or detokenization process to determine alternate user account data. For example, the originator authorizing entity computer (e.g., a first authorizing entity computer) may not be onboarded with the tokenization computer. In such a case, the
20 originator authorizing entity computer can provide first user account data that is a real account number and a tokenization flag that indicates not to tokenize the real account number (since there would be no token available). The tokenization computer may then determine, using a tokenization matrix, alternate first user account data that is the real account number, since no tokenization is to take place for the current interaction.

25 **[0044]** FIG. 1 shows a tokenization system 100 according to embodiments of the disclosure. The tokenization system 100 comprises a first user device 102, a first authorizing entity computer 104, a processing network computer 106, a tokenization computer 108, a second authorizing entity computer 110, and a second user device 112. The first user device 102 can be in operative communication with the first
30 authorizing entity computer 104, which can be in operative communication with the

processing network computer 106. The processing network computer 106 can be in operative communication with the tokenization computer 108 and the second authorizing entity computer 110, which can be in operative communication with the second user device 112.

5 **[0045]** For simplicity of illustration, a certain number of components are shown in FIG. 1. It is understood, however, that embodiments of the invention may include more than one of each component. In addition, some embodiments of the invention may include fewer than or greater than all of the components shown in FIG. 1.

10 **[0046]** Messages between at least the devices in the tokenization system 100 in FIG. 1 can be transmitted using a secure communications protocols such as, but not limited to, File Transfer Protocol (FTP); HyperText Transfer Protocol (HTTP); Secure Hypertext Transfer Protocol (HTTPS), SSL, ISO (e.g., ISO 8583) and/or the like. The communications network may include any one and/or the combination of the following: a direct interconnection; the Internet; a Local Area Network (LAN); a Metropolitan Area
15 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. The communications network can use any suitable communications protocol to generate one or more secure communication channels. A
20 communications channel may, in some instances, comprise a secure communication channel, which may be established in any known manner, such as through the use of mutual authentication and a session key, and establishment of a Secure Socket Layer (SSL) session.

25 **[0047]** The first user device 102 and the second user device 112 can include devices operated by a first user and a second user, respectively. The first user device 102, for example, can include a smartphone, a laptop, etc. The first user device 102 can be configured to initiate an interaction with a second user device 112 to obtain a resource, access to a resource, provide a resource, or provide access to a resource. The first user device 102 can connect to the first authorizing entity computer 104 via a
30 webpage or application installed on the first user device 102.

[0048] The second user device 112 can be similar to the first user device 102. In some embodiments, the second user device 112 can initiate an interaction with the first user device 102 to obtain a resource, access to a resource, provide a resource, or provide access to a resource. The second user device 112 can connect to the second
5 authorizing entity computer 110 via a webpage or application installed on the second user device 112.

[0049] The first authorizing entity computer 104 and the second authorizing entity computer 110 can include computers, server computers, databases, and/or any combination thereof to provide data between a user device (e.g., the first user device
10 102) and the processing network computer 106. In other embodiments, an authorizing entity computer can be operated by an issuing and/or authorizing entity (e.g., an issuer). An issuer can maintain an account on behalf of a user. For example, the first authorizing entity computer 104 can maintain a first account on behalf of the first user of the first user device 102. For example, the second authorizing entity computer 110 can
15 maintain a second account on behalf of the second user of the second user device 112. The first account, which is associated with the first user, can be identified by first user account data. The first user account data can be a real account number and/or a token. similarly, the second account, which is associated with the second user, can be identified by second user account data. The second user account data can be a real
20 account number and/or a token.

[0050] In some embodiments, the first authorizing entity computer 104 and the second authorizing entity computer 110 can be the same authorizing entity computer. For example, the first user of the first user device 102 can be associated with a first account maintained by the first authorizing entity computer 104, while the second user
25 of the second user device 112 can be associated with a second account maintained by the first authorizing entity computer 104.

[0051] The processing network computer 106 can include computers, server computers, databases, and/or any combination thereof to coordinate the functions of routing, generating, and formatting messages to facilitate embodiments. In other
30 embodiments, the processing network computer 106 may be in a payment processing

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

10 **[0052]** The processing network computer 106 can communicate a request message during an interaction between the first user device 102 and the second user device 112. The request message can comprise first user account data and second user account data.

15 **[0053]** In some embodiments, the processing network computer 106 can generate a tokenization request message, or receive a tokenization request message from an authorizing entity computer (e.g., the first authorizing entity computer 104), and then send the tokenization request message to the tokenization computer 108. The tokenization request message may request a token from the tokenization computer 108, and may include information including first user account data and second user account data. For example, the first user account data can be a PAN for the account to be tokenized. In some embodiments, the tokenization request message can include a first tokenization flag and a second tokenization flag that indicate whether or not to tokenize the related user account data. In other embodiments, the tokenization request message can include information regarding particular environment/circumstances in which the requested alternate user account data (e.g., a token) is to be used (e.g., during a specific time period).

25 **[0054]** After receiving the tokenization request message from the processing network computer 106, the tokenization computer 108 can select a tokenization option of a plurality of tokenization options in a tokenization matrix based on the first user account data and the second user account data. For example, the tokenization matrix

30

can include multiple tokenization options with varying inputs of first user account data, second user account data, a first tokenization flag, and a second tokenization flag. Utilizing the tokenization option that matches the data received in the tokenization request message can allow the tokenization computer to determine alternate first user account data and alternate second user account data.

[0055] The alternate user account data can be other user account data that is associated with a user account. For example, the first user account data can be a real account number while the alternate first user account data can be a token. As another example, the second user account data can be a token while the alternate second user account data can be a real account number. In some embodiments, the alternate user account data can be determined to be the same as the user account data using the selected tokenization option. For example, the first user account data can be a real account number while the alternate first user account data can be the real account number.

[0056] The tokenization computer 108 can then generate a tokenization response message comprising the alternate first user account data and the alternate second user account data, then provide the tokenization response message to the processing network computer 106.

[0057] If the alternate first user account data and/or the alternate second user account data is a token, then the tokenization computer 108 may obtain the token in any suitable manner. In some embodiments, tokens may be pre-generated by the tokenization computer 108 and stored until a request for a token is received. Once received, the real account number may be stored in a database at the tokenization computer 108 along with the token that will be associated with the real account number. In other embodiments, the token may be generated after receiving the request for the token. The token may or may not be mathematically derived from the real account number and/or any other data associated with the user account and/or the user device. In either case, the user account data (e.g., the token and the real account number), and any cryptogram (as well as any restrictions associated with the cryptogram) may be stored in a database at the tokenization computer 108, or even at the processing

network computer 106, in some embodiments. Other information that may reside in the database in the processing network computer 106 may also include balances and/or limitations associated with the token.

[0058] FIG. 2 shows a block diagram of a tokenization computer 200 according to embodiments. The exemplary tokenization computer 200 may comprise a processor 204. The processor 204 may be coupled to a memory 202, a network interface 206, a token vault 210, and a computer readable medium 208. The computer readable medium 208 can comprise tokenization matrix module 208A, a token exchange module 208B and a validation module 208C.

[0059] The memory 202 can be used to store data and code. The memory 202 may be coupled to the processor 204 internally or externally (e.g., cloud based data storage), and may comprise any combination of volatile and/or non-volatile memory, such as RAM, DRAM, ROM, flash, or any other suitable memory device. For example, the memory 202 can store first user account data, second user account data, a first tokenization flag, a second tokenization flag, a tokenization matrix, etc.

[0060] The token vault 210 may store tokens and their associated credentials (e.g., real account numbers) in a database. The database may also include cryptograms associated with the tokens, as well as any limitations on the use of such tokens or balances associated with the tokens. The token vault 210 may store data in a database such as an Oracle™ database.

[0061] The tokenization matrix module 208A may comprise code or software, executable by the processor 204, for creating and utilizing a tokenization matrix. The tokenization matrix module 208A, in conjunction with the processor 204, can generate a tokenization matrix that can indicate what outputs to determine based on input data.

The input data can include first user account data, a first tokenization flag, second user account data, and/or a second tokenization flag. The outputs determined by the tokenization matrix module 208A, in conjunction with the processor 204, can include alternate first user account data and alternate second user account data. The tokenization matrix module 208A, in conjunction with the processor 204, can generate any suitable number of tokenization matrices. For example, the tokenization matrix

module 208A, in conjunction with the processor 204, can generate a tokenization matrix for each user. In some embodiments, the tokenization matrix module 208A, in conjunction with the processor 204, can generate a tokenization matrix for each pair of users (e.g., for each originator/ receiver pair).

5 **[0062]** The tokenization matrix module 208A, in conjunction with the processor 204, can generate a tokenization matrix when a token is provisioned to a user (e.g., as described in further detail in reference to FIG. 5). As an example, the tokenization matrix module 208A, in conjunction with the processor 204 can generate a plurality of tokenization options including each variation of a first tokenization flag and a second
10 tokenization flag as well as each potential input first user account data and second user account data. For example, the tokenization matrix module 208A, in conjunction with the processor 204, can generate a first tokenization option that includes first user account data equal to a real account number, the first tokenization flag set to True, second user account data equal to a real account number, and the second tokenization
15 flag set to False. In such a case, the outputs determined using the first tokenization option may include alternate first user account data equal to a token and alternate second user account data equal to a real account number. The tokenization matrix module 208A, in conjunction with the processor 204, can generate a tokenization matrix as illustrated in FIG. 4.

20 **[0063]** The tokenization matrix module 208A, in conjunction with the processor 204, can utilize a tokenization matrix upon receiving a tokenization request message comprising first user account data and second user account data. The tokenization request message can further include a first tokenization flag. For example, a first authorizing entity computer associated with the first user device can provide the first
25 tokenization flag for a current interaction. In some embodiments, the tokenization request message can further include a second tokenization flag. For example, the first authorizing entity computer may store second tokenization flags on behalf of a second authorizing entity computer, and may provide the second tokenization flag to the tokenization computer 200 on behalf of the second authorizing entity computer.

[0064] In other embodiments, the tokenization matrix module 208A, in conjunction with the processor 204, can receive the first tokenization flag and the second tokenization flag from the first authorizing entity computer and the second authorizing entity computer prior to an interaction. The tokenization matrix module
5 208A, in conjunction with the processor 204, can utilize these first and/or second tokenization flags when the first and/or second tokenization flags are not received in the tokenization request message.

[0065] The token exchange module 208B may comprise code or software, executable by the processor 204, to cause the tokenization computer 200 to provide a
10 token in response to the receipt of a real account number, when a tokenization option of the tokenization matrix indicates the tokenization computer 200 will determine the token associated with the real account number. Furthermore, the token exchange module 208B, in conjunction with the processor 204, can provide a real account number in response to the receipt of a token, when a tokenization option of the tokenization matrix
15 indicate that the tokenization computer 200 will determine the real account number associated with the token. For example, the token exchange module 208B may contain logic that causes the processor 204 to generate a token and/or associate the token with a real account number. A token record may then be stored in a token record database and/or the token vault 210 indicating that the token is associated with a certain user or a
20 certain real account number.

[0066] The validation module 208C may comprise code or software, executable by the processor 204, to validate tokenization requests before tokens and/or a real account numbers are provided to external entities. For example, the validation module 208C may contain logic that causes the processor 204 to confirm that a tokenization
25 request message is authentic by decrypting a cryptogram included in the message, by confirming that the credentials in the tokenization request message are authentic and associated with the requesting device, and by assessing a risk associated with the requesting device.

[0067] The computer readable medium 208 may comprise code, executable by
30 the processor 204, for performing a method comprising: receiving, by a tokenization

computer from a processing network computer, a tokenization request message during an interaction between a first user device and a second user device, wherein the tokenization request message comprises first user account data and second user account data; selecting, by the tokenization computer, a tokenization option of a plurality of tokenization options in a tokenization matrix based on the first user account data and the second user account data; determining, by the tokenization computer, alternate first user account data and alternate second user account data based on the tokenization option; generating, by the tokenization computer, a tokenization response message comprising the alternate first user account data and the alternate second user account data; and providing, by the tokenization computer, the tokenization response message to the processing network computer.

[0068] In some embodiments, the tokenization computer 200 can categorize in-network message processing errors into different types. For example, a first type of in-network message processing error can include an error that could occur during tokenization (e.g., unknown account). A second type of in-network message processing error can include an error that could occur during detokenization (e.g., token not found). A third type of in-network message processing error can include restriction check failures (e.g., the interaction amount exceeds a limit, the interaction currency code is invalid, a usage number of the token has been reached, the token is expired, the token counter party check has failed, an invalid token state, etc.).

[0069] These message processing errors can be provided to an authorizing entity computer during an interaction. The authorizing entity computer can categorize the token restriction check failures into a hard rejection category or a soft rejection category. A restriction check may have a different rejection level for different interaction type (e.g., credit transfer, request for payment, remittance advice, etc.) messages and for different authorizing entity computer roles (e.g., originator or recipient) in the interaction. During the restriction checks execution, if a restriction failed with a soft reject (e.g., is categorized as a soft rejection), the restrictions check can continue executing the next restriction until all restrictions are executed or a restriction is failed with a hard reject (e.g., is categorized as a hard rejection). Each of the failure reason codes from the soft

rejections and the hard rejections can be added to a reason codes field of a response message. In some embodiments, the authorizing entity computer can provide restriction information to the tokenization computer 200 such that the tokenization computer 200 can determine perform the token restriction checks according to preferences set by the authorizing entity computer.

[0070] The network interface 206 may include an interface that can allow tokenization computer 200 to communicate with external computers. The network interface 206 may enable the tokenization computer 200 to communicate data to and from another device (e.g., a processing network computer, one or more authorizing entity computers, etc.). Some examples of the network interface 206 may include a modem, a physical network interface (such as an Ethernet card or other Network Interface Card (NIC)), a virtual network interface, a communications port, a Personal Computer Memory Card International Association (PCMCIA) slot and card, or the like. The wireless protocols enabled by the network interface 206 may include Wi-Fi™. Data transferred via the network interface 206 may be in the form of signals which may be electrical, electromagnetic, optical, or any other signal capable of being received by the external communications interface (collectively referred to as “electronic signals” or “electronic messages”). These electronic messages that may comprise data or instructions may be provided between the network interface 206 and other devices via a communications path or channel. As noted above, any suitable communication path or channel may be used such as, for instance, a wire or cable, fiber optics, a telephone line, a cellular link, a radio frequency (RF) link, a WAN or LAN network, the Internet, or any other suitable medium.

[0071] FIG. 3 shows a flowchart of an account tokenization and interaction method according to embodiments. The method illustrated in FIG. 3 will be described in the context of a first user initiating an interaction to transfer an amount to a second user. It is understood, however, that the invention can be applied to other circumstances.

[0072] At step 316, the first user device 302 can receive user input from the first user to initiate an interaction with a second user of a second user device 312. For example, the first user device 302 can receive an amount that the first user requests to

transfer to the second user. The first user can select second user account data or input second user account data associated with the second user of the second user device 312. The second user account data can include a real account number or a token.

[0073] In some embodiments, if the first user device 302 has not interacted with the second user device 312 previously, the first user can input a real account number associated with the second user device 312 (e.g., a second real account number). In other embodiments, if the first user device 302 has not interacted with the second user device 312 previously, the first user can input a token associated with the second user device 312 (e.g., a second token). The first user of the first user device 302 can obtain the second real account number or the second token from the second user in any suitable manner (e.g., spoken word, SMS message, secure data transmission, etc.).

[0074] If the first user device 302 has interacted with the second user device 312 previously, the first user device 302 can present a list of real account numbers and/or tokens that are associated with users with which the first user can interact. For example, the first user device 302 can present the second real account number or the second token to the first user (e.g., on a display) for selection.

[0075] In some embodiments, the first user device 302 can also receive a selection of which first user account data to utilize for the interaction. For example, the first user may be associated with a plurality of first user accounts that are maintained by the first authorizing entity computer 304. The first user can select which account they are requesting to utilize for the interaction. For example, the first user device 302 can present the first user with a list of real account numbers and/or tokens.

[0076] At step 318, after receiving user input to perform an interaction, the first user device 302 can generate an interaction request message comprising an amount, the first user account data, and the second user account data. In some embodiments, the first user device 302 can obtain the first user account data from memory.

[0077] At step 320, the first user device 302 can transmit the interaction request message to the first authorizing entity computer 304.

[0078] In some embodiments, after receiving the interaction request message, the first authorizing entity computer 304 can determine the first user account maintained by the first authorizing entity computer 304 using the first user account data.

[0079] At step 322, the first authorizing entity computer 304 can determine whether or not to authorize the interaction. For example, the first authorizing entity computer 304 can verify whether or not the first user account includes an amount greater than or equal to the amount included in the interaction request message. The first authorizing entity computer 304 can generate an indication of whether or not the interaction is authorized. For example, if the interaction is a data transfer, then the first authorizing entity computer 304 can determine whether or not to authorize the data transfer based on content of the data to be transferred, the amount, the data transfer history of the first user device and/or a data limit of the first user device 302.

[0080] In some embodiments, the first authorizing entity computer 304 can generate an indication of whether or not the interaction is authorized. For example, if the interaction is authorized, then the first authorizing entity computer 304 can include the indication that indicates that the interaction is authorized in the interaction request message.

[0081] In some embodiments, the first authorizing entity computer 304 can determine a first tokenization flag to include in the interaction request message. The first tokenization flag can indicate whether or not the tokenization computer 308 is to tokenize the first user account data. The first authorizing entity computer 304 can determine the first tokenization flag based on the current interaction. For example, if the interaction is the first time that the first user is interacting with the second user, then the first authoring entity computer 304 can determine to set the first tokenization flag to True (to indicate to the tokenization computer 308 to tokenize the first user account data that is the first real account number), thus increasing the security and confidentiality of the interaction.

[0082] In other embodiments, the first authorizing entity computer 304 can provide the first tokenization flag to the tokenization computer 308 prior to the current interaction. In such a case, the first tokenization flag can be a default tokenization flag

that is to be utilized if the first authorizing entity computer 304 does not provide a tokenization flag in the interaction request message.

[0083] At step 326, after authorizing the interaction, the first authorizing entity computer 304 can transmit the interaction request message to the processing network computer 306.

[0084] At step 328, after receiving the interaction request message, the processing network computer 306 can generate a tokenization request message comprising the first user data and the second user data. In some embodiments, the tokenization request message can further include a first tokenization flag. In other embodiments, the tokenization request message can further include a second tokenization flag.

[0085] At step 330, after generating the tokenization request message, the processing network computer 306 can provide the tokenization request message to the tokenization computer 308.

[0086] At step 332, after receiving the tokenization request message from the processing network computer 306, the tokenization computer 308 can select a tokenization option of a plurality of tokenization options in a tokenization matrix based on the first user account data and the second user account data. A tokenization option can include a tokenization process that may be chosen as a row in a tokenization matrix. Each tokenization option of the plurality of tokenization options can be a row in the tokenization matrix that includes one or more tokenization flags. A first tokenization option can include a first tokenization flag received from, and set by, the first authorizing entity computer 304 and a second tokenization flag received from, and set by, the second authorizing entity computer 310.

[0087] At step 334, after selecting the tokenization option, the tokenization computer 308 can determine alternate first user account data and alternate second user account data based on the tokenization option. For example, the tokenization option can indicate to the tokenization computer 308 to determine a particular alternate first user account data and a particular alternate second user account data. The

tokenization option can indicate that the alternate first user account data should be a first token (associated with the first user), while the alternate second user account data should be a second real account number (associated with the second user). As such, for example, the tokenization computer 308 can tokenize the first real account number to obtain the first token. The tokenization computer 308 can determine not to tokenize the second real account number and that the alternate second account data should be set to the second real account number.

[0088] As an illustrative example, FIG. 4 shows a tokenization matrix according to some embodiments. The tokenization matrix shown in FIG. 4 includes a plurality of rows and columns. The tokenization matrix includes the following columns: a tokenization option number 402, first user account data 404, a first tokenization flag 406, second user account data 408, a second tokenization flag 410, alternate first user account data 412, and alternate second user account data 414.

[0089] The tokenization option number 402 can be a tokenization option identifier that identifies each row (e.g., tokenization option) of the tokenization matrix.

[0090] The first user account data 404, the first tokenization flag 406, the second user account data 408, and the second tokenization flag 410 can be inputs to select a tokenization option. For example, the tokenization computer 308 can receive a tokenization request message comprising first user account data that is a first real account number, a first tokenization flag that is set to true (which indicates to tokenize the first real account number), and second user account data that is a second real account number. The tokenization computer 308 can determine the second tokenization flag that is associated with the second real account number from the database. For example, the second authorizing entity computer 310 may have previously provided the second tokenization flag to the tokenization computer 308. As an example, the second tokenization flag can be equal to True.

[0091] The tokenization computer 308 can utilize the aforementioned data to determine which tokenization option to select. In this example, the tokenization computer 308 can determine to select tokenization option number 1.

[0092] Referring back to FIG. 4, the alternate first user account data 412 and the alternate second user account data 414 can indicate, to the tokenization computer 308, which outputs to determine. For example, the first tokenization option indicates the alternate first user account data 412 to be a first token and the alternate second user
5 account data 414 to be a second token. The tokenization computer 308, after selecting the tokenization option, can determine the alternate first user account data and the alternate second user account data.

[0093] Based on the first tokenization option, the tokenization computer 308 can determine the first token as the alternate first user account data. The tokenization
10 computer 308 can determine and/or generate the first token in any suitable manner. For example, the tokenization computer 308 can retrieve the first token from the token vault or a memory. As another example, the tokenization computer 308 can generate the first token based on predetermined inputs into a cryptographic function. For example, the tokenization computer 308 can generate the first token based any
15 combination of the first real account number, a tokenization computer identifier, a first user device identifier, a first authorizing entity computer identifier, a counter, an identifier, a cryptogram, a date, a time, and/or any other suitable data associated with the first user.

[0094] Similarly, based on the first tokenization option, the tokenization computer
20 308 can determine the second token as the alternate second user account data. The tokenization computer 308 can determine and/or generate the second token in any suitable manner. The tokenization computer 308 can generate the second token in a similar or different manner to the first token.

[0095] At step 336, after determining the alternate user account data (e.g., the
25 alternate first user account data and the alternate second user account data), the tokenization computer 308 can generate a tokenization response message comprising the alternate first user account data and the alternate second user account data. In some embodiments, the tokenization response message can further include the amount, the indication of whether or not the interaction is authorized, and/or any other

suitable tokenization related data (e.g., no user found messages, tokenization failed flags, etc.).

5 **[0096]** At step 338, after generating the tokenization response message, the tokenization computer 308 can provide the tokenization response message to the processing network computer 306.

10 **[0097]** At step 340, after receiving the tokenization response message from the tokenization computer 308, the processing network computer 306 can modify the interaction request message to include the alternate first user account data and the alternate second user account data. For example, the processing network computer 306 can replace the first user account data with the alternate first user account data. The processing network computer 306 can additionally replace the second user account data with the alternate second user account data.

15 **[0098]** At step 342, after including the alternate user account data in the interaction request message, the processing network computer 306 can transmit the interaction request message to the second authorizing entity computer 310 that maintains the account identified by the alternate second user account data.

20 **[0099]** At step 344, after receiving the interaction request message, the second authorizing entity computer 310 can update the second user account associated with the second user of the second user device 312. The second authorizing entity computer 310 can update an amount of the second user account with the amount indicated in the interaction request message. For example, the second authorizing entity computer 310 can obtain the second alternate account identifier (e.g., a real account identifier) from the interaction request message, and the determine the second user account using that information prior to updating it.

25 **[0100]** At step 346, after updating the second user account, the second authorizing entity computer 310 can notify the second user of the update to the second user account. For example, the second authorizing entity computer 310 can transmit any suitable message type to the second user device 312 that includes at least the amount, and in some embodiments, the alternate first user account data.

[0101] In some embodiments, the second authorizing entity computer 310 can perform step 346 concurrently with step 344. In other embodiments, the second authorizing entity computer 310 can perform step 346 prior to step 344. For example, the second authorizing entity computer 310 can provide a notification of the interaction to the second user device 312. After the second user device 312 receives the notification, the second user can select to accept or deny the interaction. The second user device 312 can then generate a notification response that indicates whether or not the second user accepted the interaction. Once the second authorizing entity computer 310 receives the notification response, the second authorizing entity computer 310 can update the second user account at step 344 if the second user accepts the interaction.

[0102] At steps 348 and 350, a clearing and settlement process may occur. For example, at step 348, the first authorizing entity computer 304 and the processing network computer 306 can transfer funds between the computers (e.g., between accounts maintained by each respective device). For example, the first authorizing entity computer 304 can transfer an amount equal to the amount of the interaction request message, and any fees if applicable, to the processing network computer 306. At step 350, the processing network computer 306 and the second authorizing entity computer 310 can transfer funds between the computers (e.g., between accounts maintained by each respective device). For example, the processing network computer 306 can transfer an amount equal to the amount of the interaction request message to the second authorizing entity computer 310. In some embodiments, the funds provided to the second authorizing entity computer 310, during step 350, can be provided to a second user account that is associated with the second user of the second user device 312.

[0103] FIG. 5 shows a flowchart of a token initiation and interaction method according to embodiments. The method illustrated in FIG. 5 will be described in the context of a first user initiating a data transfer interaction to transfer a particular amount of data to a second user. The real account number of the first user may not yet be associated with a token. During the data transfer interaction, the first user's real

account number can be associated with a newly generated token. It is understood, however, that the invention can be applied to other circumstances.

[0104] Prior to step 514, a first user device (not shown) can initiate a data transfer to transfer an amount of data to a second user device (not shown). The first user's first user account data may not yet be associated with a token. The first user device can transmit a token provisioning request message (e.g., to request a token to be provisioned for particular first user account data) to the first authorizing entity computer 504. The token provisioning request message can include a real account number associated with the first user. This real account number can be the real account number to which the token will be assigned.

[0105] At step 514, after receiving the token provisioning request message, the first authorizing entity computer 504 can modify the token provisioning request message to include a tokenization flag. The tokenization flag can indicate whether or not user account data (e.g., the real account number) is to be tokenized during an interaction. For example, the first authorizing entity computer 504 can insert the tokenization flag into the token provisioning request message. In some embodiments, the first authorizing entity computer 504 can provide tokenization flags that indicate to tokenize any real account numbers. In other embodiments, the first authorizing entity computer 504 can provide tokenization flags that indicate not to tokenize a real account number.

[0106] As an illustrative example, the token provisioning request message may be a request message for a one-time use token to allow the first user device to perform a data transfer with the second user device one time. In such a case, the first authorizing entity computer 504 can determine that a one-time use token should be utilized with a tokenization flag that indicates to tokenize the real account number. Thus increasing the security of the one-time data transfer, since the real account number will be shielded from the second user device.

[0107] At step 516, the first authorizing entity computer 504 can provide the token provisioning request message comprising the real account number and the first tokenization flag to a tokenization computer 508.

[0108] At step 518, after receiving the token provisioning request message, the tokenization computer 508 can determine whether or not to generate the token. For example, the tokenization computer 508 can determine whether or not a token has previously been created for the real account number. The tokenization computer 508
5 can determine not to generate the token if a token has previously been generated for the real account number. In some embodiments, the tokenization computer 508 can determine to generate the token even if a previous token was already generated. For example, in some embodiments, a real account number can be associated with one or more tokens. If the tokenization computer 508 determines not to generate a token, then
10 the tokenization computer 508 can skip step 520. If the tokenization computer 508 determines to generate a token, then the tokenization computer 508 can generate the token at step 520.

[0109] At step 520, the tokenization computer 508 can generate the token associated with the real account number. The tokenization computer 508 can generate
15 the token in any suitable manner. For example, the tokenization computer 508 can generate a random number, value, string, etc. to be the token. In other embodiments, the token can be a derived value. For example, the token can be derived based on the real account number, any other user account data, a user identifier, an authorizing entity computer identifier, a tokenization computer identifier, a counter, an index, and/or a
20 cryptographic value.

[0110] At step 522, after generating the token, the tokenization computer 508 can store the token in a token vault, as described herein, or in any other secure database. The token can be stored in association with the real account number, such that the tokenization computer 508 can later determine the token based on the real account
25 number or determine the real account number based on the token. In some embodiments, the tokenization computer 508 can store the received tokenization flag as a default tokenization flag to utilize for the user device.

[0111] At step 524, in some embodiments, the tokenization computer 508 can generate a tokenization matrix. The tokenization computer 508 can generate the
30 tokenization matrix with any suitable number of new tokenization options. The

tokenization computer 508 can generate the tokenization matrix by iterating through each variation of first user account data, second user account data, a first tokenization option and a second tokenization option. For example, the tokenization computer 508 can generate the following two tokenization options, which may be the first two
5 tokenization options in the tokenization matrix (separated into inputs and outputs for ease of illustration):

[0112] Tokenization_option_1_inputs(first_user_account_data = “first real account number”, first_tokenization_flag = true, second_user_account_data = “second real account number”, second_tokenization_flag = true);

10 **[0113]** Tokenization_option_1_outputs(alternate_first_user_account_data = “first token”, alternate_second_user_account_data = “second token”);

[0114] Tokenization_option_2_inputs(first_user_account_data = “first real account number”, first_tokenization_flag = true, second_user_account_data = “second real account number”, second_tokenization_flag = false);

15 **[0115]** Tokenization_option_2_outputs(alternate_first_user_account_data = “first token”, alternate_second_user_account_data = “second real account number”).

[0116] At step 526, after generating the token, the tokenization computer 508 can generate a token provisioning response message comprising the token. In some embodiments, the token provisioning response message can comprise the token and
20 the real account number.

[0117] At step 528, after generating the token provisioning response message, the tokenization computer 508 can provide the token provisioning response message to the first authorizing entity computer 504.

[0118] At step 530, after receiving the token provisioning response message, the
25 first authorizing entity computer 504 can begin processing the data transfer to transfer data from the first user device to the second user device. In some embodiments, the first authorizing entity computer 504 can provide the token provisioning response message to the first user device. In other embodiments, the first authorizing entity

computer 504 can provide the token from the token provisioning response message to the first user device.

[0119] In some embodiments, at step 530, the first authorizing entity computer 504 and determine whether or not to authorize the data transfer based on content of the data to be transferred, the amount, the data transfer history of the first user device, a data limit of the first user device, and/or any other information and/or data stored by the first authorizing entity computer 504.

[0120] At step 532, the first authorizing entity computer 504, the processing network computer 506, the tokenization computer 508, and the second authorizing entity computer 510 can process the interaction (e.g., the data transfer) as described in FIG. 3. The steps included in step 532 are similar to the steps described in reference to FIG. 3 and will not be repeated here.

[0121] Embodiments of the disclosure have a number of advantages. The first user and the second user that perform an interaction may or may not know one another. However, during current interactions, sensitive data such as real account numbers are required to be provided to the other user in order to complete the interaction, thus compromising the confidentiality of each user. Embodiments provide advantages over previous interaction systems by maintaining confidentiality of real account numbers. During processing, the tokenization computer can determine a token for either user, or both users, of the interaction, thus hiding the real account numbers.

[0122] Doing so further provides for the advantage of increased security. For example, malicious user can attempt to fraudulently utilize received real account numbers. However, the tokenization computer can determine alternate first user account data that is a token using a tokenization option of a tokenization matrix that includes a tokenization flag that indicates to tokenize the real account number of the first user when interacting with the second user. Thus preventing the second user from receiving the first user's real account number.

[0123] Embodiments of the disclosure have a number of additional advantages. For example, a particular user (and/or an authorizing entity computer that maintains the

user's account) may not be enrolled in the tokenization service and may not yet have a token associated with a real account number. In such a case, the tokenization flag associated with the user and provided by the authorizing entity computer to the tokenization computer can indicate not to determine a token for the real account

5 number. This is beneficial since the system is agnostic of authorizing entity computer enrollment status and can still allow users to participate in peer-to-peer interactions. Further, enrollment of the users of an institution in a token service can be difficult, since it involves a significant amount of effort, and the users within a particular institution (e.g., a banking institution) to be enrolled may join or leave that institution in an unpredictable
10 manner.

[0124] Although the steps in the flowcharts and process flows described above are illustrated or described in a specific order, it is understood that embodiments of the invention may include methods that have the steps in different orders. In addition, steps may be omitted or added and may still be within embodiments of the invention.

15 **[0125]** 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, C++, C#, Objective-C, Swift, or scripting language such as Perl or Python using, for example, conventional or object-oriented techniques. The software code may be stored as a series of instructions or
20 commands on a computer readable medium for storage and/or transmission, suitable media include 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 compact disk (CD) or DVD (digital versatile disk), flash memory, and the like. The computer readable medium may be any combination of such storage or transmission devices.

25 **[0126]** Such programs may also be encoded and transmitted using carrier signals adapted for transmission via wired, optical, and/or wireless networks conforming to a variety of protocols, including the Internet. As such, a computer readable medium according to an embodiment of the present invention may be created using a data signal encoded with such programs. Computer readable media encoded with the
30 program code may be packaged with a compatible device or provided separately from

other devices (e.g., via Internet download). Any such computer readable medium may reside on or within a single computer product (e.g. a hard drive, a CD, or an entire computer system), and may be present on or within different computer products within a system or network. A computer system may include a monitor, printer, or other suitable display for providing any of the results mentioned herein to a user.

[0127] 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.

[0128] 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.

[0129] As used herein, the use of "a," "an," or "the" is intended to mean "at least one," unless specifically indicated to the contrary.

WHAT IS CLAIMED IS:

1 1. A method comprising:
2 receiving, by a tokenization computer from a processing network
3 computer, a tokenization request message during an interaction between a first user
4 device and a second user device, wherein the tokenization request message comprises
5 first user account data and second user account data;
6 selecting, by the tokenization computer, a tokenization option of a plurality
7 of tokenization options in a tokenization matrix based on the first user account data and
8 the second user account data;
9 determining, by the tokenization computer, alternate first user account
10 data and alternate second user account data based on the tokenization option;
11 generating, by the tokenization computer, a tokenization response
12 message comprising the alternate first user account data and the alternate second user
13 account data; and
14 providing, by the tokenization computer, the tokenization response
15 message to the processing network computer.

1 2. The method of claim 1, wherein the tokenization request message
2 further includes a first tokenization flag associated with the first user account data and a
3 second tokenization flag associated with the second user account data.

1 3. The method of claim 2, wherein the first user account data is a real
2 account number associated with a first user of the first user device, and wherein the first
3 tokenization flag indicates not to tokenize the real account number.

1 4. The method of claim 3, wherein determining the alternate first user
2 account data and the alternate second user account data based on the tokenization
3 option further comprises:
4 determining, by the tokenization computer, that the first user account data
5 is not to be tokenized; and
6 determining, by the tokenization computer, the alternate first user account
7 data that is the same as the first user account data.

1 5. The method of claim 1, wherein the tokenization request message
2 is received from a first authorizing entity computer via the processing network computer,
3 wherein the first authorizing entity computer is associated with the first user device and
4 is not enrolled in a tokenization program with the tokenization computer, wherein the
5 first user account data is a real account number and is not associated with a token, and
6 wherein a first tokenization flag in the tokenization request message indicates not to
7 tokenize the real account number.

1 6. The method of claim 1, wherein the first user account data is a first
2 real account number, the second user account data is a second real account number,
3 the alternate first user account data is a first token, and the alternate second user
4 account data is a second token.

1 7. The method of claim 1, wherein the tokenization request message
2 is received from an authorizing entity computer via the processing network computer,
3 wherein the first user account data is a token associated with a first user of the first user
4 device, wherein prior to receiving the tokenization request message during the
5 interaction, the method further comprises:

6 receiving, by the tokenization computer from the authorizing entity
7 computer, a token provisioning request comprising a real account number associated
8 with the first user;

9 generating, by the tokenization computer, the token associated with the
10 real account number;

11 generating, by the tokenization computer, a token provisioning response
12 message comprising the token and the real account number; and

13 providing, by the tokenization computer, the token provisioning response
14 message to the authorizing entity computer.

1 8. The method of claim 7, wherein the token provisioning request
2 further comprises a first tokenization flag that indicates whether or not to tokenize the
3 real account number during interactions, wherein the method further comprises:

4 generating, by the tokenization computer, a new tokenization option to
5 include in the tokenization matrix based on the first tokenization flag.

1 9. The method of claim 1, wherein the tokenization option includes the
2 first user account data, the second user account data, a first tokenization flag, and a
3 second tokenization flag, wherein the first tokenization flag is a first value set by a first
4 authorizing entity computer that maintains a first user account on behalf of a first user of
5 the first user device, wherein the second tokenization flag is a second value set by a
6 second authorizing entity computer that maintains a second user account on behalf of a
7 second user of the second user device.

1 10. A tokenization computer comprising:
2 a processor; and
3 a computer-readable medium coupled to the processor, the computer-
4 readable medium comprising code executable by the processor for implementing a
5 method comprising:
6 receiving, from a processing network computer, a tokenization
7 request message during an interaction between a first user device and a second
8 device, wherein the tokenization request message comprises first user account
9 data and second user account data;
10 selecting a tokenization option of a plurality of tokenization options
11 in a tokenization matrix based on the first user account data and the second user
12 account data;
13 determining alternate first user account data and alternate second
14 user account data based on the tokenization option;
15 generating a tokenization response message comprising the
16 alternate first user account data and the alternate second user account data; and
17 providing the tokenization response message to the processing
18 network computer.

1 11. The tokenization computer of claim 10 further comprising:
2 a token vault, wherein the method further comprises:

3 obtaining the tokenization matrix from the token vault.

1 12. The tokenization computer of claim 10, wherein the tokenization
2 option includes the first user account data, the second user account data, a first
3 tokenization flag, and a second tokenization flag, wherein the first tokenization flag is a
4 first value set by a first authorizing entity computer that maintains a first user account on
5 behalf of a first user of the first user device, wherein the second tokenization flag is a
6 second value set by a second authorizing entity computer that maintains a second user
7 account on behalf of a second user of a second user device.

1 13. The tokenization computer of claim 10, wherein the method further
2 comprises:
3 generating the tokenization matrix comprising the plurality of tokenization
4 options to include inputs of the first user account data, the second user account data, a
5 first tokenization flag, and a second tokenization flag.

1 14. The tokenization computer of claim 10, wherein the tokenization
2 request message further includes a first tokenization flag associated with the first user
3 account data and a second tokenization flag associated with the second user account
4 data, wherein the first user account data is a real account number associated with a first
5 user of the first user device, and wherein the first tokenization flag indicates not to
6 tokenize the real account number.

1 15. The tokenization computer of claim 10, wherein each tokenization
2 option of the plurality of tokenization options is a row in the tokenization matrix that
3 includes one or more tokenization flags.

1 16. The tokenization computer of claim 10, wherein the first user
2 account data is the same as the alternate first user account data.

1 17. A method comprising:
2 receiving, by an authorizing entity computer, an interaction request
3 message from a first user device comprising an amount, first user account data, and
4 second user account data, during an interaction between a first user and a second user;

5 determining, by the authorizing entity computer, whether or not to
6 authorize the interaction;
7 if the interaction is authorized, determining, by the authorizing entity
8 computer, a tokenization flag that indicates whether or not to tokenize the first user
9 account data;
10 modifying, by the authorizing entity computer, the interaction request
11 message to include the tokenization flag; and
12 providing, by the authorizing entity computer, the interaction request
13 message to a processing network computer, wherein the processing network computer
14 provides a tokenization request message comprising the first user account data, the
15 second user account data, and the tokenization flag to a tokenization computer, wherein
16 the tokenization computer selects a tokenization option of a plurality of tokenization
17 options in a tokenization matrix based on the first user account data and the second
18 user account data, determines alternate first user account data and alternate second
19 user account data based on the tokenization option, and generates a tokenization
20 response message comprising the alternate first user account data and the alternate
21 second user account data.

1 18. The method of claim 17, wherein the interaction request message
2 comprise an amount of funds, wherein the authorizing entity computer is a first
3 authorizing entity computer, wherein the processing network computer receives the
4 tokenization response message, modifies the tokenization response message with the
5 alternate first user account data and the alternate second user account data, and
6 provides the tokenization response message to a second authorizing entity computer,
7 wherein the method further comprises:

8 providing, by the first authorizing entity computer, the amount of funds
9 indicated in the interaction request message to the second authorizing entity computer
10 via the processing network computer using the alternate second user account data.

1 19. The method of claim 17, wherein the second user account data is
2 selected from a list of account data by the first user on the first user device, wherein the

3 first user account data is a real account number, and wherein a first tokenization flag
4 indicates not to tokenize the real account number.

1 20. The method of claim 19, wherein the interaction between the first
2 user device and a second user device is a data transfer between the first user device
3 and the second user device, wherein the amount is an amount of data to be transferred,
4 wherein determining whether or not to authorize the interaction further comprises:
5 determining, by the authorizing entity computer, whether or not to
6 authorize the data transfer based on content of the data to be transferred, the amount, a
7 data transfer history of the first user device and/or a data limit of the first user device.