TOKENIZATION REQUEST VIA ACCESS DEVICE

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of the filing date of U.S. Provisional Application No. 62/084,738, filed on November 26, 2014, which is herein incorporated by reference in its entirety for all purposes.

BACKGROUND

[0002] Tokens can be used to protect sensitive information, such as account numbers. For example, tokens may only be valid under certain circumstances, such that if a token is compromised may not pose a security threat.

[0003] However, current mechanisms for obtaining tokens are limited. For example, a mobile device may require wireless communication connectivity in order to obtain a token over the air for a specific transaction. Thus, if a mobile device is in a zone without wireless communication coverage, the mobile device may not be able to obtain a token. If the mobile device is not able to obtain a token, then an intended transaction may not be consummated. Or, the mobile device may resort to using the sensitive information to conduct the transaction, which is undesirable.

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

SUMMARY

[0005] Embodiments of the invention are directed to obtaining tokens for transactions through alternative communication channels.

[0006] One embodiment of the invention is directed to a method. The method comprises receiving, at a first computer, a credential from a user, and sending a token request message including the credential to a second computer. The token request message is in the same format as an authorization request message used to authorize a transaction. The method further comprises receiving a token associated with the credential from the second computer, generating the authorization request message, and submitting the authorization request message including the token to an authorization computer for the transaction.

[0007] Another embodiment of the invention is directed to a first computer configured to perform the above-described method.

[0008] Another embodiment of the invention is directed to a method comprising receiving, at a second computer, a token request message including a credential from a first computer. The token request message has the same format as an authorization request message used to authorize a transaction. The method further comprises validating the token request message, assigning a token to the credential, and generating a token response message including the token. The token response message has the same format as an authorization response message. The method also comprises transmitting the token response message to the first computer.

[0009] Another embodiment of the invention is directed to a second computer configured to perform the above-described method.

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

BRIEF DESCRIPTION OF THE DRAWINGS

[0011] **FIG. 1** shows a block diagram of a system for obtaining a payment token for a payment device, according to an embodiment of the invention.

[0012] **FIG. 2** shows a block diagram of an exemplary payment device according to an embodiment of the invention.

[0013] **FIG. 3** shows a block diagram of a resource provider computer according to an embodiment of the invention.

[0014] **FIG. 4** shows a block diagram of a transaction processing computer according to an embodiment of the invention.

[0015] **FIG. 5** shows a block diagram of a tokenization computer according to an embodiment of the invention.

[0016] **FIG. 6** shows a flow diagram illustrating a method for obtaining a payment token for a payment device, according to embodiments of the invention.

[0017] **FIG. 7** shows a block diagram of a system for obtaining a payment token for a mobile device, according to an embodiment of the invention.

[0018] **FIG. 8** shows a block diagram of an exemplary mobile device according to an embodiment of the invention.

[0019] **FIG. 9** shows a block diagram of a wallet provider computer according to an embodiment of the invention.

[0020] **FIG. 10** shows a flow diagram illustrating a method for obtaining a payment token for a mobile device, according to embodiments of the invention.

[0021] **FIG. 11** shows a block diagram of a computer apparatus according to an embodiment of the invention.

DETAILED DESCRIPTION

[0022] Embodiments of the present invention are directed to requesting a payment token via a merchant access device. A user can present a payment device at

an access device during a transaction. The payment device can then pass payment credentials to the access device. The payment credentials may then be sent by the access device in a token request message that is in the form of an authorization request message to a tokenization computer. The tokenization computer can respond with a token response message including a payment token that is associated with the payment credentials. The token response message may be in the form of an authorization response message. After the access device receives the payment token, it can be used to conduct the transaction instead of the payment credentials.

[0023] Some embodiments of the invention can advantageously allow normal magnetic stripe or chip type payment cards to request a payment tokens.

[0024] Some embodiments of the invention permit mobile device to obtain payment tokens via access devices. A payment token can be retrieved for a mobile device in the same manner as described above (e.g., transmit payment credentials from the mobile device to the access device, and access device sends a token request to a tokenization computer). Alternatively, the mobile device can generate the token request message and transmit the message to the access device, and then the access device can forward the token request message to the tokenization computer. Accordingly, a mobile device can obtain a payment token even when the mobile device is not in direct communication with the tokenization computer over the air.

[0025] Storing payment tokens on a payment device or mobile device can cause a security vulnerability, as the payment tokens may be compromised if the device is stolen or hacked. Instead of storing payment tokens, some embodiments of the invention allow tokens to be retrieved only when they are needed (e.g., during a transaction). Further, the payment tokens can have a short lifespan, as they may be used immediately. Accordingly, the risk of payment tokens being compromised is reduced, and any payment tokens that are stolen or lost may not pose a security threat

(e.g., because they may be no longer valid). Further, the security of requesting and providing payment tokens can be improved, as secure authorization-related encryption techniques and secure communications can be utilized.

[0026] Embodiments of the invention, as discussed herein, will primarily be described as pertaining to financial transactions and payment systems. However, embodiments of the invention can also be used in other systems. Several examples exist of applications for which it can be advantageous to use the connectivity of an access point to obtain a token instead of an over-the-air connection.

[0027] In one example, instead of obtaining a payment token via an access device for a payment transaction, it may be useful to obtain access tokens via an access point for gaining access at the access point. Access tokens can be used for physical entry into a secure area, or for digital access to secure data (e.g., an email inbox, a secure database, a restricted webpage, etc.). For example, a user may have an access card (e.g., a readable badge or mobile device) that includes access credentials for entering a restricted area. It may be desirable to protect the user's access credentials by instead utilizing an access token that represents the access credentials.

[0028] Some embodiments allow access tokens to be retrieved when the user presents the access card at an access point (e.g., an access device that may control access to a restricted area). The access point may receive the access credentials from the access card, send a token request message with the access credentials, and obtain an access token associated with the access credentials. The access point can then use the access token for determining whether to allow access to the user, and/or the access point can store the access token (e.g., instead of the access credential) in a database that records who has entered the secure area. In some embodiments, the user's access card or other access device may be able to store access tokens. Accordingly,

an access token may be stored for use at a later time. Accordingly, embodiments of the invention allow for protection of any suitable type of sensitive information by allowing for an suitable type of token to be requested and obtained.

[0029] Prior to discussing specific embodiments of the invention, some terms may be described in detail.

[0030] A "mobile device" may comprise any suitable electronic device that may be transported and 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. Examples of mobile devices include mobile phones (e.g. cellular phones), PDAs, tablet computers, net books, laptop computers, personal music players, hand-held specialized readers, etc. Further examples of mobile devices include wearable devices, such as smart watches, fitness bands, ankle bracelets, rings, earrings, etc., as well as automobiles with remote communication capabilities. A mobile device may comprise any suitable hardware and software for performing such functions, and may also include multiple devices or components (e.g. when a device has remote access to a network by tethering to another device - i.e. using the other device as a modem – both devices taken together may be considered a single mobile device).

[0031] A "payment device" may include any suitable device that may be used to conduct a financial transaction, such as to provide payment credentials to a merchant. The payment device may be a software object, a hardware object, or a physical object. As examples of physical objects, the payment device may comprise a substrate such as a paper or plastic card, and information that is printed, embossed, encoded, or otherwise included at or near a surface of an object. A hardware object can relate to

circuitry (e.g., permanent voltage values), and a software object can relate to non-permanent data stored on a device. A payment device may be associated with a value such as a monetary value, a discount, or store credit, and a payment device may be associated with an entity such as a bank, a merchant, a payment processing network, or a person. A payment device may be used to make a payment transaction. Suitable payment devices can be hand-held and compact so that they can fit into a user's wallet and/or pocket (e.g., pocket-sized). Example payment devices may include smart cards, magnetic stripe cards, keychain devices (such as the Speedpass™ commercially available from Exxon-Mobil Corp.), etc. Other examples of mobile devices include pagers, payment cards, security cards, access cards, smart media, transponders, and the like. If the payment device is in the form of a debit, credit, or smartcard, the payment device may also optionally have features such as magnetic stripes. Such devices can operate in either a contact or contactless mode. In some embodiments, a mobile device can function as a payment device (e.g., a mobile device can store and be able to transmit payment credentials for a transaction).

[0032] A "credential" may be any suitable information that serves as reliable evidence of worth, ownership, identity, or authority. A credential may be a string of numbers, letters, or any other suitable characters that may be present or contained in any object or document that can serve as confirmation.

[0033] A "value credential" may be information associated with worth. Examples of value credentials include payment credentials, coupon identifiers, information needed to obtain a promotional offer, etc.

[0034] "Payment credentials" may include any suitable information associated with 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 a

PAN (primary account number or "account number"), user name, expiration date, CVV (card verification value), dCVV (dynamic card verification value), CVV2 (card verification value 2), CVC3 card verification values, etc. CVV2 is generally understood to be a static verification value associated with a payment device. CVV2 values are generally visible to a user (e.g., a consumer), whereas CVV and dCVV values are typically embedded in memory or authorization request messages and are not readily known to the user (although they are known to the issuer and payment processors). Payment credentials may be any information that identifies or is associated with a payment account. Payment credentials may be provided in order to make a payment from a payment account. Payment credentials can also include a user name, an expiration date, a gift card number or code, and any other suitable information.

[0035] An "application" may be computer code or other data stored on a computer readable medium (e.g. memory element or secure element) that may be executable by a processor to complete a task.

[0036] A "digital wallet" can include an electronic device that allows an individual to conduct electronic commerce transactions. A digital wallet may store user profile information, payment credentials, bank account information, one or more digital wallet identifiers and/or the like and can be used in a variety of transactions, such as but not limited to eCommerce, social networks, money transfer/ personal payments, mobile commerce, proximity payments, gaming, and/or the like for retail purchases, digital goods purchases, utility payments, purchasing games or gaming credits from gaming websites, transferring funds between users, and/or the like. A digital wallet may be designed to streamline the purchase and payment process. A digital wallet may allow the user to load one or more payment cards onto the digital wallet so as to make a payment without having to enter an account number or present a physical card.

[0037] A "digital wallet provider" may include an entity, such as an issuing bank or third party service provider, that issues a digital wallet to a user that enables the user to conduct financial transactions. A digital wallet provider may provide standalone user-facing software applications that store account numbers, or representations of the account numbers (e.g., payment tokens), on behalf of a cardholder (or other user) to facilitate payments at more than one unrelated merchant, perform person-to-person payments, or load financial value into the digital wallet. A digital wallet provider may enable a user to access its account via a personal computer, mobile device or access device. Additionally, a digital wallet provider may also provide one or more of the following functions: storing multiple payment cards and other payment products on behalf of a user, storing other information including billing address, shipping addresses, and transaction history, initiating a transaction by one or more methods, such as providing a user name and password, NFC or a physical token, and may facilitate pass-through or two-step transactions.

[0038] 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.

[0039] 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 token may include a series of alphanumeric characters that may be used as a substitute for an original account identifier. For example, a token "4900 0000 0000 0001" may be used in place of a PAN "4147 0900 0000 1234." In some embodiments, a token may be "format preserving" and may have a numeric format that conforms to the account identifiers used in existing transaction 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.

[0040] "Tokenization" is a process by which data is replaced with substitute data. For example, a payment account identifier (e.g., a primary account number (PAN)) may be tokenized by replacing the primary account identifier with a substitute number (e.g. a token) that may be associated with the payment account identifier. Further, tokenization may be applied to any other information that may be replaced with a substitute value (i.e., token). Tokenization may be used to enhance transaction efficiency, improve transaction security, increase service transparency, or to provide a method for third-party enablement.

[0041] A "token provider" or "token service system" can include a system that that services payment tokens. In some embodiments, a token service system can facilitate requesting, determining (e.g., generating) and/or issuing tokens, as well as maintaining an established mapping of tokens to primary account numbers (PANs) in a repository (e.g. token vault). In some embodiments, the token service system may establish a token assurance level for a given token to indicate the confidence level of the token to PAN binding. The token service system may include or be in communication with a token vault where the generated tokens are stored. The token service system may support token processing of payment transactions submitted using tokens by de-tokenizing the token to obtain the actual PAN. In some embodiments, a token service system may include a tokenization computer alone, or in combination with other computers such as a transaction processing network computer. Various entities of a tokenization ecosystem may assume the roles of the token service provider. For example, payment networks and issuers or their agents may become the token service

provider by implementing the token services according to embodiments of the present invention.

[0042] A "token domain" may indicate an area and/or circumstance in which a token can be used. Examples of the token domain may include, but are not limited to, payment channels (e.g., e-commerce, physical point of sale, etc.), POS entry modes (e.g., contactless, magnetic stripe, etc.), and merchant identifiers to uniquely identify where the token can be used. A set of parameters (i.e. token domain restriction controls) may be established as part of token issuance by the token service provider that may allow for enforcing appropriate usage of the token in payment transactions. For example, the token domain restriction controls may restrict the use of the token with particular presentment modes, such as contactless or e-commerce presentment modes. In some embodiments, the token domain restriction controls may restrict the use of the token at a particular merchant that can be uniquely identified. Some exemplary token domain restriction controls may require the verification of the presence of a token cryptogram that is unique to a given transaction. In some embodiments, a token domain can be associated with a token requestor.

[0043] "Token expiry date" may refer to the expiration date/time of the token. The token expiry date may be passed among the entities of the tokenization ecosystem during transaction processing to ensure interoperability. The token expiration date may be a numeric value (e.g. a 4-digit numeric value). In some embodiments, the token expiry date can be expressed as an time duration as measured from the time of issuance.

[0044] A "token request message" may be an electronic message for requesting a token. A token request message may include information usable for identifying a payment account or digital wallet, and/or information for generating a payment token. For example, a token 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 service provider, a merchant identifier, a cryptogram, and/or any other suitable information. Information included in a token request message can be encrypted (e.g., with an issuer-specific key). In some embodiments, a token request message may be formatted as an authorization request message (e.g., an ISO 8583 message format). In some embodiments, the token request message may have a zero dollar amount in an authorization amount field. As another example, the token request message may include a flag or other indicator specifying that the message is a token request message.

[0045] A "token response message" may be a message that responds to a token request. A token response message may include an indication that a token request was approved or denied. A token response message may also include a payment token, mobile device identification information (e.g. a phone number or MSISDN), a digital wallet identifier, information identifying a tokenization service provider, a merchant identifier, a cryptogram, and/or any other suitable information. Information included in a token response message can be encrypted (e.g., with an issuer-specific key). In some embodiments, a token response message may be formatted as an authorization response message (e.g., an ISO 8583 message format). In some embodiments, the token response message may have a zero dollar amount in an authorization amount field. As another example, the token response message may include a flag or other indicator specifying that the message is a token response message.

[0046] 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.

[0047] A "resource provider" may be an entity that can provide a resource such as goods, services, information, and/or access. Examples of a resource provider

includes merchants, access devices, secure data access points, etc. A "merchant" may typically be an entity that engages in transactions and can sell goods or services, or provide access to goods or services.

[0048] An "acquirer" may typically be a business entity (e.g., a commercial bank) that has a business relationship with a particular merchant or other entity. Some entities can perform both issuer and acquirer functions. Some embodiments may encompass such single entity issuer-acquirers. An acquirer may operate an acquirer computer, which can also be generically referred to as a "transport computer".

[0049] 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. 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 on a user device, such as a cellular telephone, smart card, tablet, or laptop to the consumer.

[0050] An "access device" may be any suitable device that provides access to a remote system. An access device may also be used for communicating with a merchant computer, a transaction processing computer, an authentication computer, or any other suitable system. An access device may generally be located in any suitable location, such as at the location of a merchant. An access device may be in any suitable form. Some examples of access devices include POS or point of sale devices (e.g., POS terminals), cellular phones, PDAs, personal computers (PCs), tablet PCs, hand-held specialized readers, set-top boxes, electronic cash registers (ECRs), automated teller machines (ATMs), virtual cash registers (VCRs), kiosks, security systems, access systems, and the like. An access device may use any suitable contact or contactless mode of operation to send or receive data from, or associated with, a user mobile device. In some embodiments, where an access device may comprise a

POS terminal, any suitable POS terminal may be used and may include a reader, a processor, and a computer-readable medium. A reader may include any suitable contact or contactless mode of operation. For example, exemplary card readers can include radio frequency (RF) antennas, optical scanners, bar code readers, or magnetic stripe readers to interact with a payment device and/or mobile device. In some embodiments, a cellular phone, tablet, or other dedicated wireless device used as a POS terminal may be referred to as a mobile point of sale or an "mPOS" terminal.

[0051] An "authorization request message" may be an electronic message that requests authorization for a transaction. In some embodiments, it is sent to a transaction processing computer and/or an issuer of a payment card to request authorization for a transaction. An authorization request message according to some embodiments may comply with ISO 8583, which is a standard for systems that exchange electronic transaction information associated with a payment made by a user using a payment device or payment account. The authorization request message may include an issuer account identifier that may be associated with a payment device or payment account. An authorization request message may also comprise additional data elements corresponding to "identification information" including, by way of example only: a service code, a CVV (card verification value), a dCVV (dynamic card verification value), a PAN (primary account number or "account number"), a payment token, a user name, an expiration date, etc. An authorization request message may also comprise "transaction information," such as any information associated with a current transaction, such as the transaction amount, merchant identifier, merchant location, acquirer bank identification number (BIN), card acceptor ID, information identifying items being purchased, etc., as well as any other information that may be utilized in determining whether to identify and/or authorize a transaction.

[0052] An "authorization response message" may be a message that responds to an authorization request. In some cases, it may be an electronic message reply to an

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

[0053] A "server computer" may include a powerful computer or cluster of computers. For example, the server computer can be a large mainframe, a minicomputer cluster, or a group of servers functioning as a unit. In one example, the server computer may be a database server coupled to a Web server. The server computer may be coupled to a database and may include any hardware, software, other logic, or combination of the preceding for servicing the requests from one or more client computers. The server computer may comprise one or more computational apparatuses and may use any of a variety of computing structures, arrangements, and compilations for servicing the requests from one or more client computers.

[0054] **FIG. 1** shows a system **100** comprising a number of components. The system **100** comprises a payment device **115** which may be associated with a user **110** and may be able to provide payment credentials to an access device **125**. The access device **125** may be associated and in communication with a resource provider computer **130**. Further, the resource provider computer **130**, a transport computer **140**, a

transaction processing computer **150**, an issuer computer **160**, and/or a tokenization computer **170** may all be in operative communication with each other through any suitable communication channel or communications network. Suitable communications networks 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.

[0055] Messages between the computers, networks, and devices may 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), Secure Socket Layer (SSL), ISO (e.g., ISO 8583) and/or the like.

[0056] The user **110** may be able to use the payment device **115** to conduct transactions with a resource provider associated with the resource provider computer **130**. The payment device **115** may store information associated with the user **110** and/or a payment account. For example, the payment device **115** may store payment credentials as well as personal information such as a name, address, email address, phone number, or any other suitable user **110** identification information. The payment device **115** may provide this information to the access device **125** during a transaction.

[0057] **FIG. 2** shows an example of a payment device **115** in the form of a card. As shown, the payment device **115** comprises a plastic substrate **115(s)**. In some embodiments, a contactless element **115(u)** for interfacing with an access device may be present on, or embedded within, the plastic substrate **115(s)**. A magnetic stripe **115(t)** may also or alternatively be on the plastic substrate **115(s)**. User information

115(v) such as an account number, expiration date, and/or a user name may be printed or embossed on the card. In some embodiments, the payment device **115** may comprise a microprocessor and/or memory chips with user data stored in them.

[0058] Referring back to **FIG. 1**, the resource provider computer **130** may be associated with a resource provider. The resource provider may engage in transactions, sell goods or services, or provide access to goods or services to the user **110**. The resource provider may accept multiple forms of payment (e.g. the payment device **115**) and may use multiple tools to conduct different types of transactions. For example, the resource provider may operate a physical store and use the access device **125** for in-person transactions. The resource provider may also sell goods and/or services via a website, and may accept payments over the Internet. In some embodiments, the resource provider computer **130** may also be able to request payment tokens associated with the user's payment credentials.

[0059] An example of the resource provider computer **130**, according to some embodiments of the invention, is shown in **FIG. 3**. The resource provider computer **130** comprises a processor **130A**, a network interface **130B**, a transaction database **130C**, and a computer readable medium **130D**.

[0060] The computer readable medium **130D** may comprise a transaction processing module **130E**, a token request module **130F**, and any other suitable software module. The computer readable medium **130D** may also comprise code, executable by the processor **130A** for implementing a method comprising receiving, by a first computer, a credential from a user; sending a token request message including the credential to a second computer, the token request message being in the same format as an authorization request message used to authorize a transaction; receiving a token associated with the credential from the second computer; generating the

authorization request message; and submitting the authorization request message including the token to an authorization computer for the transaction.

[0061] The transaction processing module **130E** may comprise code that causes the processor **130A** to process transactions. For example, the transaction processing module **130E** may contain logic that causes the processor **130A** to receive payment credentials from the user **110** (e.g., via the access device **125** and the payment device **115**) for a transaction. The transaction processing module **130E** may be able to initiate a transaction authorization process, and may also be able to finalize a transaction so that goods and/or services can be released. In some embodiments, instead of submitting payment credentials in an authorization request upon receipt, the transaction processing module **130E** may first instruct the token request module **130F** to obtain a payment token, and then the transaction processing module **130E** may include the payment token in the authorization request message. The transaction processing module **130E** may also be able to generate transaction receipts and store transaction records (e.g., including transaction data, user information, a payment token, etc.) in the transaction database **130C**. In some embodiments, it may be beneficial to store a payment token in the transaction record instead of the user's payment credentials, as the potential of the payment credentials being compromised may thereby be reduced.

[0062] The token request module **130F** may comprise code that causes the processor **130A** to request and receive payment tokens. For example, the token request module **130F** may contain logic that causes the processor **130A** to send a token request message to a token provider. The token request message may include the user's payment credentials, resource provider identification information, and any other suitable information. The token request message may be formatted as an authorization request message, and may be transmitted along the same communication pathways as an authorization request message (e.g., it may be initially sent to the transport computer **140**).

[0063] Referring back to **FIG. 1**, in some embodiments, the access device **125** may alternatively be configured to initiate tokenization of payment credentials. For example, the access device **125** may be able to generate a token request message and send the token request message to an appropriate tokenization entity.

[0064] Authorization requests submitted by the resource provider computer **130** or the access device **125** may be sent to the transport computer **140** (which may be an acquirer computer). The transport computer **140** may be associated with the resource provider computer **130**, and may manage authorization requests on behalf of the resource provider computer **130**. The transport computer **140** may also handle token request messages on behalf of the resource provider computer **130**. For example, in some embodiments, the transport computer **140** may receive and forward token request messages in the same manner as authorization request messages.

[0065] As shown in **FIG. 1**, the transaction processing computer **150** may be disposed between the transport computer **140** and the authorizing entity computer **160**. The transaction processing computer **150** may include data processing subsystems, networks, and operations used to support and deliver authorization services, exception file services, and clearing and settlement services. For example, the transaction processing computer **150** may comprise a server coupled to a network interface (e.g., by an external communication interface), and databases of information. The transaction processing computer **150** may be representative of a transaction processing network. An exemplary transaction processing network may include VisaNet™. Transaction 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 transaction processing computer **150** may use any suitable wired or wireless network, including the Internet.

[0066] An example of the transaction processing computer **150**, according to some embodiments of the invention, is shown in **FIG. 4**. The transaction processing computer **150** comprises a processor **150A**, a network interface **150B**, a transaction database **150C**, and a computer readable medium **150D**.

[0067] The computer readable medium **150D** may comprise a transaction processing module **150E**, a token request module **150F**, and any other suitable software module. The computer readable medium **150D** may also comprise code, executable by the processor **150A** for implementing a method comprising receiving, by a transaction processing computer, a token request message including a credential (e.g., a value credential) from a first computer, wherein the token request message is in the same format as an authorization request message used to authorize a transaction; transmitting the token request message to a second computer; receiving a token response message including a token associated with the credential from the second computer, wherein the token response message is in the same format as an authorization response message; transmitting the token response message to the first computer; receiving the authorization request message from the first computer for the transaction, the authorization request message including the token; transmitting the authorization request message to an authorization computer; receiving the authorization response message from the authorization computer, the authorization response message indicating that the transaction is authorized; and transmitting the authorization response message to the first computer.

[0068] The transaction processing module **150E** may comprise code that causes the processor **150A** to process transactions. For example, the transaction processing module **150E** may contain logic that causes the processor **150A** to analyze transaction risk, and to forward, authorize, or reject authorization request messages for payment transactions. The transaction processing module **150E** may also be able to store transaction records in the transaction database **150C**. For example, the transaction

database **150C** may include a record of each completed transaction that includes transaction details (e.g. items purchased, amount, timestamp), resource provider information, user **110** information (e.g. a name, a phone number and/or other contact information, a payment token, an expiration date, etc.), and/or any other suitable information.

[0069] The token request module **150F** may comprise code that causes the processor **150A** to process token requests. For example, the token request module **150F** may contain logic that causes the processor **150A** to receive and forward token request messages and token response messages. In some embodiments, the token request module **150F** may handle token request messages similarly to authorization request messages. For example, the token request module **150F** may receive a token request message from the transport computer **140**, identify a set of payment credentials within the message, identify an authorizing entity associated with the payment credentials, and then forward the token request message to the authorizing entity computer **160**. Thus token request messages may be forwarded to the authorizing entity computer **160** or another relevant tokenization entity along the same communication channels as an authorization request message.

[0070] Referring back to **FIG. 1**, the transaction processing computer **150**, the transport computer **140**, and the authorizing entity computer **160** may operate suitable routing tables to route authorization request messages and/or token request messages using payment credentials, payment tokens, and/or other suitable identifiers.

[0071] The authorizing entity computer **160** may issue and manage a payment account and an associated payment device **115** of the user **110**. The authorizing entity computer **160** may be able authorize transactions that involve the payment account. Before authorizing a transaction, the authorizing entity computer **160** may authenticate payment credentials received in the authorization request, and check that there is

available credit or funds in an associated payment account. The authorizing entity computer **160** may also receive and/or determine a risk level associated with the transaction, and may weigh the risk when deciding whether or not to authorize the transaction. If the authorizing entity computer **160** receives an authorization request that includes a payment token, the authorizing entity computer **160** may be able to de-tokenize the payment token in order to obtain the associated payment credentials.

[0072] The tokenization computer **170** (which may also be referred to as a "token provider computer") may be able to provide payment tokens. For example, a token request message may be sent to the tokenization computer **170**, and the tokenization computer **170** may then generate and/or associate a payment token with payment credentials in the token request message. In embodiments, tokenization services may be provided by the authorizing entity computer **160**, the transaction processing computer **150**, the transport computer **140**, a third-party service provider, or any other suitable entity. Thus, the tokenization computer **170** may be incorporated as a part of another entity in the system **100**. In some embodiments, as shown in **FIG. 1**, the tokenization computer **170** may be a separate entity.

[0073] An example of the tokenization computer **170**, according to some embodiments of the invention, is shown in **FIG. 5**. The tokenization computer **170** comprises a processor **170A**, a network interface **170B**, a token record database **170C**, and a computer readable medium **170D**.

[0074] The computer readable medium **170D** may comprise a tokenization module **170E**, a detokenization module **170F**, a security module **170G**, and any other suitable software module. The computer readable medium **170D** may also comprise code, executable by the processor **170A** for implementing a method comprising receiving, at a second computer, a token request message including a credential from a first computer, the token request message being in the same format as an authorization

request message used to authorize a transaction; validating the token request message; assigning a token to the credential; generating a token response message including the token, the token response message being in the same format as an authorization response message; and transmitting the token response message to the first computer.

[0075] The tokenization module **170E** may comprise code that causes the processor **170A** to provide payment tokens. For example, the tokenization module **170E** may contain logic that causes the processor **170A** to generate a payment token and/or associate the payment token with a set of payment credentials. A token record may then be stored in the token record database **170C** indicating that the payment token is associated with a certain user **110** or a certain set of payment credentials. The tokenization module **170E** may be able to send a token response message including the payment token along communication rails normally used for authorization response messages.

[0076] The detokenization module **170F** may comprise code that causes the processor **170A** to detokenize payment tokens. For example, the detokenization module **170F** may contain logic that causes the processor **170A** to identify a token record associated with a payment token in the token record database **170C**. A set of payment credentials associated with the payment token (as indicated in the token record) can then be identified. In some embodiments, the detokenization module **170F** may detokenize a payment token in response to a detokenization request message (e.g., received from the authorization entity computer **160**, the transaction processing computer **150**, or any other suitable entity).

[0077] The security module **170G** may comprise code that causes the processor **170A** to validate token requests before a payment token is provided. For example, security module **170G** may contain logic that causes the processor **170A** to confirm that

a token request message is authentic by decrypting a cryptogram included in the message, by confirming that the payment credentials are authentic and associated with the requesting user **110**, by assessing risk associated with the requesting resource provider computer **130**, or by using any other suitable information. If the payment credentials are encrypted, the security module **170G** may be able to decrypt the encrypted payment credentials (e.g. via an issuer-specific key).

[0078] As shown and described with respect to **FIG. 1**, the system **100** allows tokens to be request through alternative communication channels, such as authorization rails. In some embodiments, an entity that sends a token request message may be referred to as a "first computer." Accordingly, the resource provider computer **130** and/or the access device **125** could be considered examples of a first computer. In some embodiments, an entity that provides tokens may be referred to as a "second computer." Accordingly, the tokenization computer **170** could be considered an example of a second computer.

[0079] A method **600** according to embodiments of the invention can be described with respect to **FIG. 6**. In the method illustrated in **FIG. 6**, credentials may be passed from the payment device **615** to the access device **625** to initiate the token request process and the payment transaction process. The method in **FIG. 6** advantageously allows payment devices such as magnetic stripe cards to be used in a tokenization process, even though such payment devices have limited functionality. The steps shown in the method **600** may be performed sequentially or in any suitable order in embodiments of the invention. In some embodiments, one or more of the steps may be optional.

[0080] The user may wish to purchase a good or service from the resource provider. At step **S602**, in order to perform the purchase, the user may provide payment credentials (e.g. via the payment device **615**) to the access device **625**. For

example, in some embodiments, the user may swipe a magnetic stripe card at the access device **625**, or the user may present a smart card with contactless communication capabilities (e.g. NFC, Bluetooth, RF, etc.) to the access device **625**. The payment device **615** may provide a PAN, a security code, an expiration date, a name, an address, a phone number, and/or any other suitable payment credentials.

[0081] At step **S604**, the resource provider computer **630** may receive (e.g. via the access device **625** or an online webpage) the payment credentials. In some embodiments, the resource provider computer **630** may then encrypt the payment credentials. For example, the resource provider computer **630** may encrypt the payment credentials with an issuer-specific key. Alternatively, in some embodiments, the resource provider computer **630** may encrypted payment credentials that are already encrypted. For example, the payment device **615** may use an issuer-specific key to encrypt the payment credentials, and may transmit the encrypted payment credentials to the access device **625**. Accordingly, the resource provider computer **630** may not have access to sensitive unencrypted payment credentials.

[0082] At step **S606**, the resource provider computer **630**, may determine that a payment token may be requested for the payment credentials. For example, in some embodiments, the resource provider computer **630** may recognize that the payment credentials include a PAN and not a payment token. The first six digits of a PAN may include a BIN, so if a valid BIN is present in the payment credentials, then it may be determined that the payment credentials include a PAN. In some embodiments, a payment token may be requested for certain types of payment devices **615**, such as payment devices **615** that are associated with a certain authorizing entity computer **660** or transaction processing computer **650**.

[0083] At step **S608**, the resource provider computer **630** may send a token request message to the transport computer **640**. The token request message may

include the payment credentials, which may be encrypted. The token request message may also include transaction information, a merchant ID, a cryptogram, a digital certificate (e.g., which may be signed by a key held by the resource provider computer **630**), and/or any other suitable information. In some embodiments, the token request message may have an indication that it was sent by the resource provider computer **630** on behalf of the user, and may include any suitable user information.

[0084] The token request message may be transmitted through channels typically used for authorization request messages, and/or the token request message may be formatted similarly to an authorization request message. For example, the token request message may have an ISO 8583 message format. Also, the token request message may be a zero-dollar or no amount authorization request message. Similar to how an authorization request message can be forwarded, at step **S610**, the transport computer **640** may forward the token request message to the transaction processing computer **650**. Further, at step **S612**, the transaction processing computer **650** may forward the token request message to the authorizing entity computer **660** associated with the payment credentials. In some embodiments, the transaction processing computer **650** may also analyze risk associated with the request and/or perform any other suitable checks and processing before forwarding the token request message.

[0085] At step **S614**, the authorizing entity computer **660** may forward the token request message to the tokenization computer **670**. The authorizing entity computer **660** may forward the message after determining that the received message is a token request message and not an authorization request message (e.g., based on an indicator that it is a token request, based on a lack of transaction-related information such as a transaction amount).

[0086] At step **S616**, the tokenization computer **670** may validate the token request message (e.g. based on a cryptogram, transaction information, merchant

information, the payment credentials, or any other suitable information in the token request message). In some embodiments, the tokenization computer **670** may use an encryption key to validate a digital certificate included in the token request message. If the payment credentials are encrypted, the tokenization computer **670** may be able to decrypt the encrypted payment credentials (e.g. via an issuer-specific key). In some embodiments, the authorizing entity computer **660** may decrypt the payment credentials before forwarding the token request message to the tokenization computer **670**.

[0087] At step **S618**, the tokenization computer **670** may generate a payment token and/or create an association between the payment token and the payment credentials. In some embodiments, the tokenization computer **670** may instead identify an existing payment token that is already associated with the payment credentials.

[0088] At step **S620**, the tokenization computer **670** may send a token response message to the authorizing entity computer **660**. The token response message may include the payment token as well as transaction information, a merchant ID, a cryptogram, and/or any other suitable information.

[0089] Similar to the token request message described above, the token response message may be transmitted through channels typically used for authorization response messages, and/or the token response message may be formatted similarly to an authorization response message. For example, similar to how an authorization response can be forwarded, at step **S622**, the authorizing entity computer **660** may forward the token response message to the transaction processing computer **650**. Also, at step **S624**, the transaction processing computer **650** may forward the token response message to the transport computer **640**. Further, at step **S626**, the transport computer **640** may forward the token response message to the resource provider computer **630**.

[0090] At step **S628**, the resource provider computer **630** (or the access device **625**) may receive the token response message including the payment token. In some

embodiments, at this point, the resource provider computer **630** may erase any record of the payment credentials, such that the payment credentials are not stored at the resource provider computer **630**. Then, the payment token may be used in place of the payment credentials (e.g. for transaction authorization and record-keeping purposes).

[0091] Although the example above describes the resource provider computer **630** generating a token request message and receiving a token response message, in other embodiments, the access device **625** may alternatively perform the above-described functions performed by the resource provider computer **630**.

[0092] Thus, a request for a payment token associated with the payment device **615** may be sent by the resource provider computer **630** or the access device **625** on behalf of the user, allowing a payment card to be usable within a tokenization system. In some embodiments, having obtained the payment token, the transaction can then proceed to be completed using the payment token instead of the payment credentials.

[0093] At step **S630**, the resource provider computer **630** (or the access device **625**) may send an authorization request message for the transaction to the transport computer **640**. In some embodiments, the authorization request message may include the payment token instead of the payment credentials. The authorization request message may also include transaction information (e.g. items purchased, amount, etc.), merchant information (e.g. merchant name, location, etc.), and any other suitable information.

[0094] At step **S632**, the transport computer **640** may forward the authorization request message to the transaction processing computer **650**. At step **S634**, the transaction processing computer **650** may forward the authorization request message to the authorizing entity computer **660**.

[0095] At step **S636**, the authorizing entity computer **660** may detokenize the payment token and obtain the payment credentials. For example, the authorizing entity

computer **660** may obtain the payment credentials from the tokenization computer **670** or from a local token record database. In some embodiments, any other suitable entity may instead detokenize the payment token. For example, the transaction processing computer **650** may detokenize the payment token before forwarding the authorization request message to the authorizing entity computer **660**.

[0096] At step **S638**, the authorizing entity computer **660** may authorize or reject the transaction based on the payment credentials. For example, the authorizing entity computer **660** may identify the payment account associated with the payment credentials and/or payment token, and may determine whether there are sufficient funds.

[0097] At step **S640**, the authorizing entity computer **660** may send an authorization response indicating whether or not the transaction was authorized to the transaction processing computer **650**. The authorization response message may include the payment token, transaction details, merchant information, and any other suitable information. In some embodiments, in order to protect the payment credentials by limiting exposure, the authorization response message may not include the payment credentials.

[0098] At step **S642**, the transaction processing computer **650** may forward the authorization response message to the transport computer **640**. At step **S644**, the transport computer **640** may forward the authorization response message to the resource provider computer **630**.

[0099] At step **S646**, the resource provider computer **630** may release the purchased goods and/or services to the user based on the authorization response message. Further, the resource provider computer **630** may store a transaction record including the payment token, user information, transaction details, and any other suitable information. In some embodiments, the resource provider computer **630** may

erase any sensitive information, such as the encrypted or unencrypted payment credentials, but the resource provider computer **630** may store remaining information, such as the payment token.

[0100] Embodiments of the invention allow a number of alternatives to various aspects of the method **600**. For example, in some embodiments, step **S606** and other token requesting steps may be performed by the access device **625**. For example, the access device **625** may include instructions for tokenization, or the access device **625** can interface with a resource provider system that can determine whether or not to request a payment token. Further, although the authorizing entity computer **660** in **FIG. 6** obtains a token from the tokenization computer **670** and communicates with it to detokenize the token, in other embodiments, these functions may be performed by the transport computer **640** and/or the transaction processing computer **650** (as illustrated in **FIG. 1**).

[0101] As described above, the method **600** advantageously allows the token request message to be sent via channels typically used for authorization request messages, allowing for efficient transmission and utilization of existing pathways. The token request message may be routed to the tokenization computer **670** via a number of entities. For example, as described above, the token request message may be forwarded via the transport computer **640**, the transaction processing computer **650**, and/or the authorizing entity computer **660**.

[0102] In some embodiments, the token request message may be forwarded directly to the tokenization computer **670**. For example, as shown in **FIG. 1**, the token request message may be sent directly to the tokenization computer **670** after reaching the transport computer **640**, the transaction processing computer **650**, the authorizing entity computer **660**, or any other suitable entity. In some embodiments, once the token request message is recognized as a token request instead of an authorization request

(e.g., by the transport computer **640**), the token request may be sent directly to the tokenization computer **670**. Further, as described above, in some embodiments the tokenization computer **670** may be embodied as part of another entity, such as the transport computer **640**, the transaction processing computer **650**, the authorizing entity computer **660**. Thus, the token request message may have reached its destination once it arrives at whichever entity is providing the tokenization services.

[0103] Similarly, the token response message may be sent via channels typically used for authorization response messages, allowing for efficient transmission and utilization of existing pathways. The token request message may be routed to the resource provider computer **630** via a number of entities. In some embodiments, as shown in **FIG. 1**, the tokenization computer **670** may send the token response message directly to the transport computer **140**, the transaction processing computer **650**, and/or any other suitable entity.

[0104] In some embodiments, there limits may be placed on the payment token provided in the method **600**. For example, the token domain and/or the token expiration date may be configured such that the payment token may only be usable in a certain area (e.g. based on geo-location data), at the resource provider computer **630** (e.g. based on a merchant ID), for the amount of the current transaction, and/or for a certain time period. Also, the payment token may be a one-time use token, and it may only be eligible for the current transaction. In some embodiments, the payment token may be utilized for a purchase immediately after being requested, and accordingly it may be assigned a short lifespan (e.g. it may have an expiration time in the near future). For example, the payment token may only be valid for 1 hour, 10 minutes, 5 minutes, 1 minute, 30 seconds, or any other suitable amount of time. In some embodiments, payment token parameter specifications may be requested in the token request message, or there may be specific rules for tokens associated with the authorizing entity computer **660** or any other suitable entity.

[0105] In some embodiments, instead of a magnetic stripe card or smart card, the user may use a different mode of payment, such as a mobile device. The following description relates to embodiments where a mobile device or any other suitable device with increased functionality is used for providing payment during a transaction.

[0106] **FIG. 7** shows a system **700** comprising a number of components, according to embodiments of the invention. The system **700** may be similar to the system **100**, but some components may be different. For example, instead of the payment device **115**, system **700** may comprise a mobile device **720**. Also, instead of the tokenization computer **170**, system **700** may comprise a wallet provider computer **780**. Similar to the system **100**, in the system **700**, the access device **725** may be associated with and in communication a resource provider computer **730**. Further, the resource provider computer **730**, a transport computer **740**, a transaction processing computer **750**, an authorizing entity computer **760**, and/or the wallet provider computer **780** may all be in operative communication with each other through any suitable communication channel or communications network.

[0107] The user **710** may be able to use the mobile device **720** to conduct transactions with a resource provider associated with the resource provider computer **730**. The mobile device **720** may store information associated with the user **710** and/or a payment account. For example, the mobile device **720** may store (e.g., in a secure element) or have access to payment credentials as well as personal information such as a name, address, email address, phone number, or any other suitable user **710** identification information (e.g., via a digital wallet application). The mobile device **720** may be able to provide this information to the access device **725** during a transaction (e.g., via Bluetooth, NFC, RF, or any other suitable type of short range communications). Further, the mobile device **720** may be capable of more complex functions, such as generating request messages and receiving communications from

various entities, such as the access device **725** and/or the wallet provider computer **780**.

[0108] An example of the mobile device **720**, according to some embodiments of the invention, is shown in **FIG. 8**. Mobile device **720** may include circuitry that is used to enable certain device functions, such as telephony. The functional elements responsible for enabling those functions may include a processor **720A** that can execute instructions that implement the functions and operations of the device. Processor **720A** may access memory **720E** (or another suitable data storage region or element) to retrieve instructions or data used in executing the instructions, such as provisioning scripts and mobile applications. Data input/output elements **720C**, such as a keyboard or touchscreen, may be used to enable a user to operate the mobile device **720** and input data (e.g., user authentication data). Data input/output elements may also be configured to output data (via a speaker, for example). Display **720B** may also be used to output data to a user. Communications element **720D** may be used to enable data transfer between mobile device **720** and a wired or wireless network (via antenna **720H**, for example) to assist in connectivity to the Internet or other network, and enabling data transfer functions. Mobile device **720** may also include contactless element interface **720F** to enable data transfer between contactless element **720G** and other elements of the device, where contactless element **720G** may include a secure memory and a near field communications data transfer element (or another form of short range communications technology). As noted, a cellular phone or similar device is an example of a mobile device **720** that may be used in accordance with embodiments of the present invention. However, other forms or types of devices may be used without departing from the underlying concepts of the invention. For example, the mobile device **720** may alternatively be in the form of a payment card, a key fob, a tablet computer, a wearable device, a vehicle such as a car, etc.

[0109] The memory **720E** may comprise a digital wallet application **720J**, a tokenization module **720L**, and any other suitable module or data. The mobile device **720** may have any number of mobile applications installed or stored on the memory **720E** and is not limited to that shown in **FIG. 7**. The memory **720E** may also comprise code, executable by the processor **720A** for implementing a method comprising generating, by the mobile device, a token request message including a credential, the token request message being in the same format as an authorization request message used to authorize a transaction; sending the token request message to a first computer, wherein the first computer sends the token request message to a second computer, and wherein the first computer receives a token response message including a token associated with the credential from the second computer; receiving the token response message from the first computer; and providing the token to the first computer as payment for a transaction, wherein the first computer submits the authorization request message including the token to an authorization computer for the transaction.

[0110] The digital wallet application **720J** may provide a user interface for the user **710** to provide input and initiate, facilitate, and manage transactions using the mobile device **720**. The digital wallet application **720J** may be able to store and/or access a payment token and/or payment credentials. The digital wallet application **720J** may also store an issuer-specific key, or any other suitable encryption means. The digital wallet application **720J** may be able to cause the mobile device **720** to transmit the payment token and/or payment credentials in any suitable manner (e.g., NFC, QR code, etc.). In some embodiments, in order to increase security, payment tokens and/or payment credentials may not be stored at the mobile device **720**. Instead, the payment tokens and/or payment credentials can be temporality retrieved from the wallet provider computer **780** when a transaction is being performed.

[0111] The digital wallet application **720J** may be associated with and/or provided by the wallet provider computer **780**, the authorizing entity computer **760**, an issuer-

trusted third party, the transaction processing computer **750**, the transport computer **740**, the resource provider computer **730**, or any other suitable entity.

[0112] The tokenization module **720L** may be a module of the digital wallet application **720J** or a separate application on the mobile device **120**. The tokenization module **720L** may comprise code that causes the processor **720A** to obtain payment tokens. For example, the tokenization module **720L** may contain logic that causes the processor **720A** to request a token from the wallet provider computer **780** or any other suitable tokenization service provider (e.g., the authorizing entity computer **760** or the transaction processing computer **750**). In some embodiments, the mobile device **120** may be able to communicate over-the-air with the wallet provider computer **780**, and thus the tokenization module **720L** may be able to send a direct request to the wallet provider computer **780**. In some embodiments, the tokenization module **720L** may be able to send a token request message to the wallet provider computer **780** via communication channels typically used for authorization messages. For example, the tokenization module **720L** may cause the mobile device **720** to send a token request message to the access device **725**, and the request may be forwarded through the authorization rails to the wallet provider computer **780**.

[0113] As mentioned, tokenization services may be provided by the wallet provider computer **780**, the authorizing entity computer **760**, the transaction processing computer **750**, the transport computer **740**, or any other suitable entity. The wallet provider computer **780** may additionally be able to provide other digital wallet-related services. For example, the wallet provider computer **780** may provide a digital wallet application, store payment credentials, store transaction records, and perform any other suitable transaction-related services. The wallet provider computer **780** may be associated with and/or in communication with one or more of the resource provider computer **730**, the transport computer **740**, the transaction processing computer **750**, and the authorizing entity computer **760**.

[0114] An example of the wallet provider computer **780**, according to some embodiments of the invention, is shown in **FIG. 9**. The wallet provider computer **780** comprises a processor **780A**, a network interface **780B**, a user database **780C**, and a computer readable medium **780D**.

[0115] The computer readable medium **780D** may comprise a tokenization module **780E**, a detokenization module **780F**, a security module **780G**, and any other suitable software module. The computer readable medium **780D** may also comprise code, executable by the processor **780A** for implementing a method comprising receiving, at a second computer, a token request message including a credential from a first computer, the token request message being in the same format as an authorization request message used to authorize a transaction; validating the token request message; assigning a token to the credential; generating a token response message including the token, the token response message being in the same format as an authorization response message; and transmitting the token response message to the first computer.

[0116] The tokenization module **780E** may comprise code that causes the processor **780A** to provide payment tokens. For example, tokenization module **780E** may contain logic that causes the processor **780A** to generate a payment token and/or associate the payment token with a set of payment credentials. A token record may then be stored in the user database **780C** indicating that the payment token is associated with a certain user **710**, a certain set of payment credentials, or a certain digital wallet. The tokenization module **780E** may be able to send a token response message including the payment token along communication rails normally used for authorization response messages.

[0117] The detokenization module **780F** may comprise code that causes the processor **780A** to detokenize payment tokens. For example, the detokenization

module **780F** may contain logic that causes the processor **780A** to identify a token record associated with a payment token in the user database **780C**. A set of payment credentials associated with the payment token (as indicated in the token record or digital wallet) can then be identified. In some embodiments, the detokenization module **780F** may detokenize a payment token in response to a detokenization request message (e.g., received from the authorization entity computer **760**, the transaction processing computer **750**, or any other suitable entity).

[0118] The security module **780G** may comprise code that causes the processor **780A** to validate token requests before a payment token is provided. For example, security module **780G** may contain logic that causes the processor **780A** to confirm that a token request message is authentic by decrypting a cryptogram included in the message, by confirming that the payment credentials are authentic and associated with the requesting user **710**, by checking that the use of payment tokens is approved for an associated digital wallet, by assessing risk associated with the requesting resource provider computer **730**, or by using any other suitable information. If the payment credentials are encrypted, the security module **780G** may be able to decrypt the encrypted payment credentials (e.g. via an issuer-specific key).

[0119] Similar to **FIG. 1**, various entities in **FIG. 7** could be referred to as a first computer or a second computer. For example, the resource provider computer **730** and/or the access device **725** could be considered examples of a first computer, and the wallet provider computer **780** could be considered an example of a second computer.

[0120] A method **1000** according to embodiments of the invention can be described with respect to **FIG. 10**. In the method **1000** illustrated in **FIG. 10**, a mobile device **1020** may use authorization communication channels to obtain and load a token thereon. Once the mobile device **1020** contains the token, it can be used at any suitable resource provider (e.g., any suitable merchant), and not just the resource

provider that was used to obtain the token for the mobile device **1020**. Some elements in other Figures are also referred to. The steps shown in the method **1000** may be performed sequentially or in any suitable order in embodiments of the invention. In some embodiments, one or more of the steps may be optional.

[0121] The user may wish to purchase a good or service from the resource provider. The user may wish to use the mobile device **1020** for providing payment. In some embodiments, in order to avoid compromise of payment information, the mobile device **1020** may not store payment credentials and/or payment tokens. Instead, the mobile device **1020** may wait until a transaction is about to take place before it retrieves a payment token from the wallet provider computer **1080**. However, there may not always be a sufficient over-the-air connection (e.g., cellular or Wi-Fi) for the mobile device **1020** to communicate with the wallet provider computer **1080**. Accordingly, the mobile device **1020** may instead leverage the resource provider's ability to communicate with the wallet provider computer **1080** via normal authorization channels.

[0122] At step **S1002**, the mobile device **1020** may activate a digital wallet application and/or a payment function. For example, the user may select a payment function in order to pay for the transaction.

[0123] At step **S1004**, the mobile device **1020** may generate a token request message (e.g., in response to a payment function being activated). The token request message may include payment information (e.g. a PAN, security code, expiration date, name, address, and/or phone number), information identifying the wallet provider computer **1080**, and any other suitable information. Alternatively, in some embodiments, the token request message may not include payment credentials in order to protect the sensitive data. Instead, the token request message may include a digital wallet identifier, mobile device identifier, or any other suitable information that can be used to identify the user's digital wallet or payment account.

[0124] In some embodiments, the some or all of the information included in the token request message may be encrypted with an issuer-specific key. Further, the token request message may include a cryptogram, a digital certificate (e.g., which may be signed by a key held by the mobile device **1020**), and/or any other security-related information.

[0125] At step **S1006**, the mobile device **1020** may transmit the token request message to the access device **1025** (e.g., via NFC, Bluetooth, RF, etc.). For example, the user may hold the mobile device **1020** near enough to the access device **1025** so that they can communicate wirelessly.

[0126] At step **S1008**, the resource provider computer **1030** may receive (e.g. via the access device **1025**) the token request message. In some embodiments, the token request message may include encrypted payment credentials or no payment credentials, and thus the resource provider computer **1030** may not have access to sensitive unencrypted payment credentials.

[0127] At step **S1010**, the resource provider computer **1030** may determine that the token request message should be sent to the wallet provider computer **1080**. For example, the token request message may be formatted as an authorization request message (e.g., an ISO 8583 message format) such that the resource provider computer **1030** can determine that the message should be forwarded along as an authorization request message. The resource provider computer **1030** may also detect a flag or indicator in the token request message specifying that the token request message should be forwarded. Additionally, the resource provider computer **1030** may optionally add transaction information, a merchant ID, a cryptogram, a digital certificate (e.g., which may be signed by a key held by the resource provider computer **1030**), and/or any other suitable information to the token request message.

[0128] At steps **S1012**, **S1014**, **S1016**, and **S1018**, the token request message may be forwarded to the transport computer **1040**, to the transaction processing computer **1050**, authorizing entity computer **1060**, and then the wallet provider computer **1080**. Thus, the token request message may be transmitted through channels typically used for authorization request messages.

[0129] In some embodiments, the transaction processing computer **1050** and/or the authorizing entity computer **1060** may also analyze risk associated with the request and/or perform any other suitable checks and processing before forwarding the token request message. Further, the authorizing entity computer **1060** may forward the message to the wallet provider computer **1080** after determining that the received message is a token request message. For example, the authorizing entity computer **1060** may determine that the token request message includes an token request indicator, that the token request message lacks transaction-related information such as a transaction amount (or it includes a zero or no-dollar amount), or that the token request message lacks payment credentials.

[0130] At step **S1020**, the wallet provider computer **1080** may authenticate the token request message and/or the requesting digital wallet application. For example, the token request message may be validated based on a cryptogram, merchant information, the payment credentials, transaction information, or any other suitable information in the token request message. In some embodiments, the wallet provider computer **1080** may use an encryption key to validate a digital certificate included in the token request message. In some embodiments, the wallet provider computer **1080** may open a secure and private channel between the wallet provider computer **1080** and the mobile device **1020**. This may enable mobile security checks (e.g. by the security module **780G**) and token provisioning functions to occur. These functions may involve multiple communications/messages being sent between the mobile device **320** and the wallet provider server computer **380**.

[0131] At step **S1022**, the wallet provider computer **1080** may identify the payment account and/or payment credentials for which a token is being requested. For example, if the payment credentials are included in the token request message, the wallet provider computer **1080** can locate the payment credentials within the message. If the payment credentials are encrypted, the wallet provider computer **1080** may be able to decrypt them (e.g. via an issuer-specific key). In some embodiments, the authorizing entity computer **1060** may decrypt the payment credentials before forwarding the token request message to the wallet provider computer **1080**.

[0132] Alternatively, in some embodiments, the wallet provider computer **1080** may identify the user's record or the user's digital wallet (e.g., in the user database **780C**) based on other information in the token request message, such as a digital wallet identifier, mobile device identifier, or any other suitable information. Then, a set of payment credentials can be obtained from the identified digital wallet.

[0133] At step **S1024**, the wallet provider computer **1080** may generate a payment token and/or create an association between the payment token and the payment credentials. In some embodiments, the wallet provider computer **1080** may instead identify an existing payment token that is already associated with the payment credentials. In some embodiments, as already described above for the method **600**, there may be limits placed in the token domain and/or the token expiration date of the payment token.

[0134] At step **S1026**, the wallet provider computer **1080** may generate and send a token response message to the authorizing entity computer **1060**. The token response message may include the payment token as well as transaction information, a merchant ID, a cryptogram, a digital wallet application identifier, a mobile device identifier, and/or any other suitable information. Some or all of the information included in the token response message may be encrypted with an issuer-specific key. The

token response message may have an ISO 8583 message format, and/or the token response message may be formatted as a zero or no-dollar authorization response message.

[0135] At steps **S1028**, **S1030**, **S1032**, and **S1034**, the token response message may be forwarded to the transaction processing computer **1050**, to the transport computer **1040**, to the resource provider computer **1030**, and then to the access device **1025**. Thus, token response message may be transmitted through channels typically used for authorization response messages.

[0136] In some embodiments, the token response message may be routed to the access device **1025** in a different manner. For example, as shown in **FIG. 7**, the wallet provider computer **1080** may send the token response message directly to the transport computer **1040**, the transaction processing computer **1050**, and/or any other suitable entity.

[0137] At step **S1036**, the access device **1025** may send the token response message to the mobile device **1020**. For example the user may still be holding the mobile device **1020** in within communication proximity of the access device **1025**, or the user may be prompted to hold out the mobile device **1020** again.

[0138] At step **S1038**, the mobile device **1020** may associate the payment token with the digital wallet application or a certain set of payment credentials. The payment token may be stored at the mobile device **1020**, or it may be deleted after being used for a transaction.

[0139] Thus, the mobile device **1020** may successfully leverage the connectivity of an access device **1025** for obtaining a payment token from the wallet provider computer **1080** via authorization communication channels. Accordingly, the mobile device **1020** can obtain payment tokens in real time during a transaction, and the mobile device **1020** can obtain payment tokens even when other wireless communication

services (e.g., 3G, LTE, Wi-Fi) are unavailable. After receiving the payment token, the digital wallet application on the mobile device **1020** may then be able to use the payment token for the current transaction.

[0140] At step **S1040**, the mobile device **1020** may transmit the payment token to the access device **1025** as payment for the transaction. For example, the user may continue to hold the mobile device **1020** near the access device **1025** so that communication (e.g., NFC, Bluetooth, RF, etc.) is possible. Alternatively, the access device **1025** may prompt the user to provide payment information (e.g., raise the mobile device **1020** again) after the token requesting process was completed. Note that since the mobile device **1020** is now loaded with a payment token, it can use that payment token at any other suitable access device at any other suitable resource provider and not just at the access device **1025**.

[0141] At step **S1042**, the access device **1025** may forward the payment token to the resource provider computer **1030** for processing. The access device **1025** may also provide transaction details and any other suitable information.

[0142] At step **S1044**, the resource provider computer **1030** (or the access device **1025**) may send an authorization request message for the transaction to the transport computer **1040**. In some embodiments, the authorization request message may include the payment token instead of the payment credentials. The authorization request message may also include transaction information (e.g. items purchased, amount, etc.), merchant information (e.g. merchant name, location, etc.), and any other suitable information.

[0143] At step **S1046**, the transport computer **1040** may forward the authorization request message to the transaction processing computer **1050**. At step **S1048**, the transaction processing computer **1050** may forward the authorization request message to the authorizing entity computer **1060**.

[0144] At step **S1050**, the authorizing entity computer **1060** may detokenize the payment token and obtain the payment credentials. For example, the authorizing entity computer **1060** may obtain the payment credentials from the wallet provider computer **1080**, from a local token record database, or from any other suitable token provider. In some embodiments, any other suitable entity may instead detokenize the payment token. For example, the transaction processing computer **1050** may detokenize the payment token before forwarding the authorization request message to the authorizing entity computer **1060**.

[0145] At step **S1052**, the authorizing entity computer **1060** may authorize or decline the transaction based on the payment credentials. For example, the authorizing entity computer **1060** may identify the payment account associated with the payment credentials and/or payment token, and may determine whether there are sufficient funds.

[0146] At step **S1054**, the authorizing entity computer **1060** may send an authorization response indicating whether or not the transaction was authorized to the transaction processing computer **1050**. The authorization response message may include the payment token, transaction details, merchant information, and any other suitable information. In some embodiments, in order to protect the payment credentials by limiting exposure, the authorization response message may not include the payment credentials.

[0147] At step **S1056**, the transaction processing computer **1050** may forward the authorization response message to the transport computer **1040**. At step **S1058**, the transport computer **1040** may forward the authorization response message to the resource provider computer **1030**.

[0148] At step **S1060**, the resource provider computer **1030** may release the purchased goods and/or services to the user based on the authorization response

message. Further, the resource provider computer **1030** may store a transaction record including the payment token, user information, transaction details, and any other suitable information. In some embodiments, the resource provider computer **1030** may erase any sensitive information, such as the encrypted or unencrypted payment credentials, but the resource provider computer **1030** may store remaining information, such as the payment token.

[0149] Embodiments of the invention allow a number of alternatives to various aspects of the method **1000**. For example, in some embodiments, step **S1010** and other token requesting steps may be performed by the access device **1025**.

[0150] Additionally, in some embodiments, the token request message may be forwarded more directly to the wallet provider computer **1080**. For example, as shown in **FIG. 7**, the token request message may be sent directly to the wallet provider computer **1080** after reaching the transport computer **1040**, the transaction processing computer **1050**, the authorizing entity computer **1060**, or any other suitable entity. In some embodiments, once the token request message is recognized as a token request instead of an authorization request (e.g., by the transport computer **1040**), the token request may be sent directly to the wallet provider computer **1080**.

[0151] Further, as described above, in some embodiments the wallet provider computer **1080** may be embodied as part of another entity, such as the transport computer **1040**, the transaction processing computer **1050**, the authorizing entity computer **1060**. Thus, the token request message may have reached its destination once it arrives at whichever entity is providing the tokenization services. The token request message may include a recipient identifier (e.g. a wallet provider ID or an issuer ID), such that the message can be directed to the appropriate recipient.

[0152] As described above in the method **1000**, one or more communications can take place between the mobile device **1020** and the access device **1025**. In some

embodiments, the total time needed for communications between the mobile device **1020** and the access device **1025** (e.g., sending a token request, receiving a token response, providing payment, and/or receiving a transaction receipt) may be 30 seconds, 10 seconds, 5 seconds, 3 seconds, 1 second, or any other suitable amount of time. The time may vary from transaction to transaction. The user may hold the mobile device **1020** at or near the access device **1025** while the communications are taking place, and may remove the mobile device **1020** when the communications are finished.

[0153] In some embodiments, the user may be informed of communication progress and/or when it is acceptable to remove the mobile device **1020**. For example, the access device **1025** and/or the mobile device **1020** may provide an indication when the communications are completed, such as an audible sound, a vibration, an electric pulse, and/or a displayed message.

[0154] Embodiments of the invention have a number of advantages. For example, in embodiments of the invention, payment devices such as credit cards can be integrated and used in payment systems that involve tokenization. Accordingly, users that do not have a mobile device or that are accustomed to a certain type of payment device (e.g. magnetic stripe credit cards) can participate in tokenization systems. Thus, a transition is provided from previous payment systems without tokenization to new payment systems with tokenization. Also, security may be increased for purchases made with payment devices such as credit cards, because a token can be provided and stored instead of sensitive payment information (e.g. a PAN).

[0155] Another advantage is that it may be easy for users to obtain tokens. The user might simply present a payment card or mobile device at an access device, and a token may be retrieved and then used for a purchase. Accordingly, the token requesting process may be seamless or undetected to the user.

[0156] Additionally, a mobile device may be able to obtain tokens when the mobile device does not have any connectivity (e.g. cell service, Wi-Fi, etc.). A merchant access device can essentially act as connectivity point (which is secure and reliable) through which the mobile device can request and receive tokens.

[0157] Further, tokens may only be valid for a short time duration because tokens may be used for a purchase immediately after being received. Accordingly, security may be increased, because if a token is compromised it may not be usable for fraudulent transactions at a later time. Also, devices that might retrieve and store tokens ahead of time (e.g. mobile devices, smart cards, etc.) may no longer need to store tokens, because tokens can be obtained during a transaction. Tokens stored on devices can be vulnerable because small devices are easily lost, and the tokens are often only protected by software. Accordingly, reducing the amount of time a token spends on a device before being used can reduce the risk of tokens being stolen or compromised.

[0158] **FIG. 11** is a high-level block diagram **12** of a computer system that may be used to implement any of the entities or components described above. The subsystems shown in **FIG. 11** are interconnected via a system bus **75**. Additional subsystems include a printer **74**, keyboard **78**, storage device **79**, and monitor **76**, which is coupled to display adapter **82**. Peripherals and input/output (I/O) devices, which couple to I/O controller **71**, can be connected to the computer system by any number of means known in the art, such as a serial port. For example, I/O port **77** or external interface **81** 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 **75** allows the central processor **73** to communicate with each subsystem and to control the execution of instructions from system memory **72** or the storage device **79**, as well as the exchange of information between subsystems. The system memory **72** and/or the storage device may embody a computer-readable medium.

[0159] Other embodiments of the invention are also contemplated.

[0160] One embodiment of the invention is directed to a method comprising receiving, at a second computer, a token request message including a credential from a first computer, the token request message being in the same format as an authorization request message used to authorize a transaction; validating, by the second computer, the token request message; assigning, by the second computer, a token to the credential; generating, by the second computer, a token response message including the token, the token response message being in the same format as an authorization response message; and transmitting, by the second computer, the token response message to the first computer.

[0161] Another embodiment of the invention is directed to a second computer configured to perform the above-described method. In some embodiments, the second computer may be a tokenization computer and/or a wallet provider computer.

[0162] Another embodiment of the invention is directed to a method comprising generating, by a mobile device, a token request message including a credential, the token request message being in the same format as an authorization request message used to authorize a transaction; sending, by the mobile device, the token request message to a first computer, wherein the first computer sends the token request message to a second computer, and wherein the first computer receives a token response message including a token associated with the credential from the second computer; receiving, by the mobile device, the token response message from the first computer; and providing, by the mobile device, the token to the first computer as payment for a transaction, wherein the first computer submits the authorization request message including the token to an authorization computer for the transaction.

[0163] Another embodiment of the invention is directed to a mobile device configured to perform the above-described method.

[0164] Another embodiment of the invention is directed to a method comprising receiving, by an intermediary computer, a token request message including a credential from a first computer, the token request message being in the same format as an authorization request message used to authorize a transaction; transmitting, by the intermediary computer, the token request message to a second computer; receiving, by the intermediary computer, a token response message including a token associated with the credential from the second computer, the token response message being in the same format as an authorization response message; transmitting, by the intermediary computer, the token response message to the first computer; receiving, by the intermediary computer, the authorization request message from the first computer for the transaction, the authorization request message including the token; transmitting, by the intermediary computer, the authorization request message to an authorization computer; receiving, by the intermediary computer, the authorization response message from the authorization computer, the authorization response message indicating that the transaction is authorized; and transmitting, by the intermediary computer, the authorization response message to the first computer.

[0165] Another embodiment of the invention is directed to an intermediary computer configured to perform the above-described method. In some embodiments, the intermediary computer may be a transport computer or a transaction processing computer.

[0166] As described, the inventive service may involve implementing one or more functions, processes, operations or method steps. In some embodiments, the functions, processes, operations or method steps may be implemented as a result of the execution of a set of instructions or software code by a suitably-programmed computing device, microprocessor, data processor, or the like. The set of instructions or software code may be stored in a memory or other form of data storage element which is accessed by the computing device, microprocessor, etc. In other embodiments, the

functions, processes, operations or method steps may be implemented by firmware or a dedicated processor, integrated circuit, etc.

[0167] 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.

[0168] While certain exemplary embodiments have been described in detail and shown in the accompanying drawings, it is to be understood that such embodiments are merely illustrative of and not intended to be restrictive of the broad invention, and that this invention is not to be limited to the specific arrangements and constructions shown and described, since various other modifications may occur to those with ordinary skill in the art.

[0169] As used herein, the use of "a", "an" or "the" is intended to mean "at least one", unless specifically indicated to the contrary.

WHAT IS CLAIMED IS:

1. A method comprising:

receiving, at a first computer, a credential from a user;

sending, by the first computer, a token request message including the credential to a second computer, the token request message being in the same format as an authorization request message used to authorize a transaction, wherein the token request message passes through an acquirer computer before the token request message is received by the second computer;

receiving, at the first computer, a token associated with the credential from the second computer;

generating, by the first computer, the authorization request message; and

submitting, by the first computer, the authorization request message including the token to an authorization computer for the transaction.

2. The method of claim 1, wherein the first computer is an access device.

3. The method of claim 1, wherein the token request message is formatted as an ISO 8583 message.

4. The method of claim 1, wherein the token is valid for 1 minute, 5 minutes, or 1 hour.

5. The method of claim 1, wherein the credential is encrypted.

6. The method of claim 1, wherein the credential is received by the first computer from a magnetic stripe card.

7. The method of claim 1, wherein the credential is received by the first computer from a mobile device.

8. The method of claim 7, wherein a mobile device identifier is also received from the mobile device, and wherein the token request message further includes the mobile device identifier.

9. The method of claim 7, further comprising:

sending, by the first computer, the token to the mobile device; and then

receiving, at the first computer, the token from the mobile device for use with the transaction.

10. A first computer comprising:

a processor; and

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

receiving a credential from a user;

sending a token request message including the credential to a second computer, the token request message being in the same format as an authorization request message used to authorize a transaction, wherein the token request message passes through an acquirer computer before the token request message is received by the second computer;

receiving a token associated with the credential from the second computer;

generating the authorization request message; and

submitting the authorization request message including the token to an authorization computer for the transaction.

11. The first computer of claim 10, wherein the first computer is an access device.

12. The first computer of claim 10, wherein the authorizing computer receives the authorization request message, obtains the credential associated with the

token, and authorizes the transaction based on an account associated with the credential.

13. The first computer of claim 10, wherein the first computer is a resource provider computer, and wherein the second computer is a token provider computer.

14. The first computer of claim 10, further comprising:

receiving an authorization response message indicating that the transaction is authorized; and

storing a transaction record including the token, and not including the credential.

15. The first computer of claim 10, wherein the credential is received from a magnetic stripe card.

16. The first computer of claim 10, wherein the credential is received from a mobile device.

17. The first computer of claim 16, wherein the credential received from the mobile device is received along with a request for a token.

18. The first computer of claim 16, further comprising:

sending the token to the mobile device; and then

receiving the token from the mobile device for use with the transaction.

19. The method of claim 1, wherein the token request message comprises an amount data field with a zero-dollar amount or no amount.

20. The method of claim 1, wherein the token request message includes a flag specifying that the token request message is a token request message.

21. The first computer of claim 10, wherein the token request message is formatted as an ISO 8583 message.